Universidad de Valladolid

Facultad de **Derecho**

Grado en **Derecho**

Doctrina jurisprudencial sobre diligencias de investigación tecnológicas

Presentado por:

Rocío Largo Chamorro

Tutelado por:

Alejandro Hernández López

Valladolid, 25 de junio de 2020

RESUMEN

El presente trabajo estudia las diferentes diligencias de investigación tecnológica, reguladas en la LECrim a raíz de la reforma llevada a cabo por la LO 13/2015, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, y de la doctrina jurisprudencial sobre esta materia del Tribunal Supremo, del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos, que hasta la llegada de la reforma ha ido supliendo la laguna legislativa existente sobre esta materia. Se analiza también la incidencia que supone cada una de ellas sobre los derechos fundamentales del investigado, como el derecho al secreto de las comunicaciones, el derecho a la intimidad y a la propia imagen y el derecho a la inviolabilidad del domicilio del art. 18 CE y, por consiguiente, la necesidad, salvo excepciones, de la autorización judicial correspondiente para su adopción, y de su control judicial posterior.

Palabras clave: diligencias de investigación tecnológicas, derechos fundamentales, garantías procesales, control judicial, doctrina jurisprudencial.

ABSTRACT

The aim of this work is to evaluate the different records of technological research, regulated in the LECrim as a result of the reform carried out by the LO 13/2015, for the strengthening of the procedural guarantees and the regulation of the technological research measures, and of the jurisprudential doctrine on this matter of the Supreme Court, the Constitutional Court and the European Court of Humans Rights, that until the arrival of the reform has been filling the legislative gap on this matter. The impact of each of them on the fundamental rights of the individual has been also evaluated, as well as the right to confidentiality of communication, the right to privacy and self-image and the right to inviolability of the home (art.18 CE), and therefore the need of a legal authorization for its adoption and later judicial control, with a few exceptions.

Key words: technological investigative measures, fundamental rights, procedural guarantees, judicial control, jurisprudential doctrine.

ABREVIATURAS

ART.	Artículo
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
GPS	Global Positioning System (Sistema de Posicionamiento Global)
IMEI	International Mobile Station Equipment Identity (Identidad internacional de equipo móvil)
IMSI	International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil)
IP	Internet Protocol (Protocolo de Internet)
LECRIM	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
SAP	Sentencia de la Audiencia Provincial
SJP	Sentencia del Juzgado de lo Penal
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STSJ	Sentencia del Tribunal Superior de Justicia
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo

ÍNDICE

1. INTRODUCCIÓN

El presente trabajo tiene como objeto de estudio las diligencias de investigación tecnológica que regula la Ley de Enjuiciamiento Criminal, apoyándose para su explicación en la doctrina jurisprudencial.

En primer lugar, y a modo de introducción, voy a hablar de la reforma de la LECrim llevada a cabo por la LO 13/2015, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Debe darse esta importancia a la reforma puesto que ha suplido el gran vacío normativo que existía con anterioridad debido a los grandes avances tecnológicos que han surgido en los últimos años y al uso, cada vez más generalizado, de la tecnología y la informática.

En este sentido se había manifestado en varias ocasiones el TEDH, que requería una regulación clara y precisa a la hora de acordar estas diligencias, dada su gran injerencia en los derechos fundamentales de la persona investigada, concretamente los derechos del artículo 18 CE y 8 CEDH.

Posteriormente haré referencia a los requisitos que han de cumplir todas y cada una de estas medidas para que puedan ser practicadas por la Policía Judicial, que necesitarán en la mayoría de los casos, ser acordadas por la autoridad judicial competente, siendo esta quien se encargue de determinar el alcance de la medida, entre otros aspectos, cumpliendo con los requisitos establecidos por la ley, y con los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

Después, centraré mi atención en la explicación de cada una de estas medidas de investigación tecnológicas, que son, la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Y para finalizar, haré referencia a la figura del agente encubierto informático, que se regula separadamente a estas diligencias anteriormente mencionadas pero que se trata también de una medida de investigación que ha ido adquiriendo importancia en los últimos años.

2. ANTECEDENTES Y LIMITACIÓN A LOS DERECHOS FUNDAMENTALES

2.1. Situación y regulación de las medidas de investigación tecnológicas antes de la reforma de la LECrim.

Como sabemos, a lo largo de los años, las nuevas tecnologías han estado cada vez más presentes en muchos ámbitos de nuestras vidas, han ido evolucionando con una gran rapidez, y, por supuesto, también se han visto presentes en la comisión y en la persecución de delitos. Muestra de ello es la proliferación y regulación en la LECrim de las llamadas medidas de investigación tecnológicas, cuestión que estudiaremos detalladamente en este trabajo.

Las nuevas tecnologías se empezaron a utilizar para cometer nuevos delitos y eso hizo que fuese necesaria la utilización de nuevas formas de investigación para poder responder a ellos de la manera más acorde posible, y así es como las medidas de investigación tecnológicas se fueron introduciendo poco a poco en este ámbito.

Estas medidas de investigación han sido introducidas en la Ley de Enjuiciamiento Criminal gracias a la reforma efectuada por la LO 13/2015, pero lo cierto es que ya existían y ya se hacía uso de ellas con anterioridad, y es aquí donde surgió el problema, puesto que antes del año 2015 encontramos un gran vacío normativo en lo que concierne a su regulación y a las garantías exigibles para su autorización y práctica.

Antes de esta reforma de la LECrim, nos encontrábamos ante una situación de escasa regulación en lo que se refiere a las medidas de investigación tecnológicas, y no solo eso, sino que cada vez que la tecnología avanzaba, el problema se iba agravando aún más. Las nuevas tecnologías cada vez eran más utilizadas para la perpetración de delitos y para su investigación, y se carecía de una norma habilitante que permitiera hacer uso de estas diligencia. Este vacío normativo se ha ido salvando durante años por la jurisprudencia, intentando así "salvar la inconstitucionalidad por omisión, lo que el Tribunal Europeo de Derechos Humanos ha calificado en varias ocasiones como lesivo del principio de legalidad y del derecho a la intimidad y secreto de las comunicaciones"[1].

El uso de estos medios de investigación tecnológica sin una norma que los habilite, ha hecho que el TEDH se pronunciara sobre la materia y condenara a España y a otros muchos países por esta falta de regulación, sobre todo en lo que se refiere a interceptación de las comunicaciones telefónicas, que cada vez eran más frecuentes.

[1] ASENCIO MELLADO, José María. *Derecho procesal penal.* Valencia: Tirant lo Blanch, 2019, p. 232.

En este sentido, ya desde hacía años, este Tribunal venía reiterando, como podemos observar en la famosa sentencia de 24 de abril de 1990, casos *Huvig Kruslin c. Francia*[2], que "las medidas de investigación que pudieran incidir en el ámbito de la intimidad del investigado debían estar previstas en la ley". Además, el Tribunal introdujo el concepto de calidad de ley, con el que se pretende que el individuo conozca cuando el estado podía restringir sus derechos, y evitar también situaciones de abuso del estado[3].

Asimismo, una de las sentencias del TEDH más características, que denunciaba esta carencia de regulación, es la sentencia de 30 de julio de 1988, caso *Valenzuela Contreras contra España*. En ella, se cuestionaba la vulneración del artículo 8 CEDH[4] por la interceptación de unas líneas telefónicas, sin estar prevista esta medida en una ley suficientemente previsible y clara. El TEDH falló a favor del demandante, afirmando la violación del artículo mencionado, alegando que en el momento de las escuchas "el Derecho español, escrito y no escrito, no indicaba con suficiente claridad el alcance y las modalidades del ejercicio de las facultades discrecionales de las autoridades en el ámbito considerado"[5].

El TEDH exigía sin duda una modificación legislativa que también se ve reflejada en la sentencia de 26 de Septiembre de 2006, caso *Abdulkadir Cobán c. España*[6] y en la sentencia de 18 de febrero de 2003, Caso *Prado Bugallo c. España*, en la que también el Tribunal condenó a España por la vulneración de este artículo 8 CEDH, ya que considera que "las garantías introducidas por la Ley de 1988 no responden a todas las condiciones exigidas por la jurisprudencia del Tribunal"[7].

---

[2] STEDH de 24 de abril de 1990, *caso Kruslin c. Francia*, CE:ECHR:1990:0424JUD001180185; STEDH de 24 de abril de 1990, *caso Huvig c. Francia*, CE:ECHR:1990:0424JUD001110584.

[3] Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal (BOE n.º 70 de 22 de marzo de 2019).

[4] Artículo 8 CEDH Artículo 8 CEDH "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[5] STEDH de 30 de julio de 1988, *caso Valenzuela Contreras c. España,* CE:ECHR:1998:0730JUD002767195 FJ. 61.

[6] STEDH de 26 de Septiembre de 2006, caso *Abdulkadir Cobán c. España*, CE:ECHR:2006:0925DEC001706002

[7] STEDH de 18 de febrero de 2003*, caso Prado Bugallo c. España*, CE:ECHR:2003:0218JUD005849600.

2.2. Reforma de la LECrim, efectuada por la LO 13/2015, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.

La LO 13/2015, de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, cumplió al fin con las exigencias del TEDH y procedió a la reforma de la LECrim tan necesaria y esperada. Esta ley entró en vigor el 6 de diciembre de 2015 y ha supuesto una auténtica revolución en la materia que nos ocupa, adaptando la legislación a la nueva situación y a los avances tecnológicos que habían tenido lugar, e introduciendo nuevos medios de investigación tecnológica.

Muchas de estas medidas de investigación ya existían y se practicaban con anterioridad a la reforma, pero como ya he mencionado anteriormente, se llevaban a cabo sin una base legal clara, que debía ser integrada por la jurisprudencia, por lo que era obvia la necesidad de esta reforma. Otras, en cambio, ya estaba reguladas con anterioridad, como es el caso de las interceptaciones telefónicas, pero que igualmente necesitaban de esta reforma para ser adaptadas a la situación actual.

Como ya he expuesto en el epígrafe anterior, los avances tecnológicos comenzaron a usarse también en la comisión de delitos, por lo que, evidentemente, era necesaria una respuesta acorde con esta nueva delincuencia, y una regulación a la altura de la situación. Además, es importante mencionar que de la misma forma que esta nueva delincuencia afecta a derechos fundamentales de las personas, también lo hacen estas medidas y actos de investigación tecnológica, por lo que esta reforma de LECrim era completamente necesaria para que se pudiera actuar cumpliendo todas las garantías procesales que se requiere.[8]

La reforma operada por la LO 13/2015 se ocupa de poner fin al vacío normativo existente hasta ese momento, en lo que se refiere a estas diligencias de investigación tecnológicas, y proporciona los instrumentos necesarios para actuar en este ámbito con todas las garantías procesales exigibles y cumpliendo con todos y cada uno de los principios rectores, a los que posteriormente haré referencia. La reforma se centra además en indicar todos los requisitos que ha de cumplir la resolución judicial que habilite cada una de estas diligencias, limitando su ámbito objetivo de aplicación, su duración y otros aspectos.

En primer lugar, se introduce un capítulo, concretamente el capítulo IV del título VIII, que establece unas disposiciones comunes a las distintas medidas de investigación tecnológicas y que aclara cuáles son los principios rectores y las garantías que han de estar

[8] MONTERO AROCA, Juan. Derecho jurisdiccional III. Proceso penal. Valencia: Tirant lo Blanch, 2019.

presentes en la práctica de estas medidas. Posteriormente, en los capítulos siguientes, se establece la regulación específica y singular de cada una de estas medidas de investigación tecnológicas.

En definitiva, la LO 13/2015 no solo trata de establecer una serie de disposiciones comunes, sino que fija una regulación específica para cada una de diligencias de investigación tecnológica, adaptando nuestra legislación a la realidad actual, se pone fin a una carente legislación, como así llevaba exigiendo el TEDH a través de sus condenas, y se establece un régimen jurídico claro y preciso que ha de interpretarse en el sentido más favorable a la garantía de estos derechos fundamentales.

2.3. ¿Cómo afectan estas medidas de investigación tecnológicas a los derechos fundamentales?

La LECrim regula, en su título VIII del Libro II, las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución,

Se deduce de ello que las medidas de investigación que están reguladas en dicho título producen la injerencia, en mayor o en menor medida, en los derechos fundamentales previstos en el artículo 18CE. Este artículo de nuestro texto constitucional establece que

> "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Dentro de estas medidas limitativas de los derechos del artículo 18 CE, hemos de distinguir, por un lado, las diligencias de investigación que podríamos calificar como "tradicionales", como son la entrada y registro en lugar cerrado, el registro de libros y papeles y la detención y apertura de la correspondencia escrita y telegráfica, de las diligencias de investigación tecnológica, que van a ser el objeto de estudio en el presente trabajo. Estas últimas son la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de imagen, seguimiento y localización y

captación de la imagen, el registro de dispositivos de almacenamiento masivo de información, y los registros remotos sobre equipos informáticos.

La incidencia de estas diligencias de investigación en derechos fundamentales del investigado, tan importantes como la intimidad, el secreto de las comunicaciones o la inviolabilidad del domicilio, ha hecho que se trabajara tanto por conseguir una regulación lo bastante clara y suficiente sobre el alcance y control de estas medidas, objetivo que se consiguió con la reforma de la LECrim.

3. LAS MEDIDAS DE INVESTIGACION TECNOLÓGICAS

3.1. Disposiciones comunes a las medidas de investigación tecnológicas.

3.1.1. Regulación legal

Para comenzar el estudio de las medidas de investigación tecnológicas, hay que hacer referencia a un nuevo capítulo de la LECrim, el Capítulo IV del Título VIII del Libro II, introducido con la reforma, y denominado "Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos", que concretamente se corresponde con los artículos 588 bis a) al 588 bis k).

En estos artículos se recoge un catálogo de disposiciones comunes aplicables a todas las medidas de investigación tecnológica y se regulan una serie de cuestiones formales, como la solicitud de prórroga, las reglas generales de duración, el secreto, el control de la medida, la afectación a terceras personas, la utilización de información en procedimiento distinto, el cese de la medida y la destrucción de registros.

Este capítulo se introduce en la ley con la intención de regular las condiciones y los presupuestos comunes que legitiman dichas medidas, pero sin entrar a fondo en ninguna de ellas, ya que "cada diligencia modulará algunos de estos aspectos y se regirá por las reglas específicas propias de su particularidad"[9].

[9] Preámbulo IV. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Antes de entrar en el estudio de los principios rectores por los que se rige esta materia que nos ocupa, he de mencionar que el uso de estas medidas de investigación tecnológicas ha de tener lugar durante la instrucción de las causas, como así nos indica expresamente el artículo 588 bis a) LECrim, sin perjuicio de que alguna pueda ser utilizada durante la fase de investigación preprocesal, pero en ningún caso, se podrá recurrir a ellas en otros momentos ni con fines distintos.

3.1.2. Principios rectores

Este nuevo capítulo IV comienza con el artículo 588 bis a, por el cual se requiere que, como norma general, medie autorización judicial a la hora de adoptar estas medidas de investigación tecnológicas, y, además, se requiere que la autorización se dicte con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Del desarrollo de este artículo se deduce que toda medida en la que no se observe alguno de estos principios será inadmisible, puesto que todos y cada uno de ellos deben cumplirse, como así ha reiterado el Tribunal Constitucional en varias de sus sentencias, que, además, ha considerado estos principios como determinantes de la validez del acto de injerencia[10].

Respecto al primero de ellos, el principio de especialidad, y atendiendo a lo dispuesto en el apartado 2 de este artículo 588 bis a, hay que decir que la medida ha de estar relacionada con la investigación de un delito concreto, y que queda prohibido autorizar medidas que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

De este artículo se desprende que, para cumplir con este principio de especialidad, el objeto de la medida ha de ser el esclarecimiento de un hecho punible concreto. Esto no quiere decir que los hechos que se descubran con la investigación tengan que ser idénticos a los hechos investigados, puesto que contamos con que el objeto del proceso no responde a una imagen fija[11] y pueden cambiar las circunstancias ya previstas de comisión del delito, pero sí que va a ser necesario que el acuerdo de la medida esté vinculado con un delito concreto, que tendrá que ser determinado con anterioridad a la resolución judicial habilitante. Por consiguiente, se entiende que todas las medidas de investigación tecnológica de naturaleza prospectiva están prohibidas, entendiéndose por ellas las que se adoptan para buscar pruebas sin que tengan relación con un caso concreto.

---

[10] *Vid.* STC 70/2002, de 3 de abril. ES:TC:2002:70.

[11] *Cfr*: STS 412/2011, de 11 de mayo. ES: TS: 2011:3088. F.6.B.

En esta línea se ha mantenido el Tribunal Supremo a lo largo de los años y así lo ha reiterado en varias ocasiones. Concretamente las sentencias 276/96 de 2 de abril, 792/2007 de 30 de mayo, 457/2010 de 25 de mayo, 426/2016 de 19 de mayo y 71/2017, de 8 de febrero son un claro ejemplo de ello[12]. En ellas, el TS se ha pronunciado aclarando ciertas cuestiones sobre la materia, entre las que cabe destacar, que "el principio de especialidad impone la prohibición de intervenciones prospectivas, mediante las que los poderes públicos se inmiscuyen en la intimidad del sospechoso con el exclusivo objeto de indagar qué es lo que encuentran", y que este principio "exige que la decisión jurisdiccional de intervención de las comunicaciones telefónicas éste siempre relacionada con la investigación de un delito concreto cuyos elementos ya se dibujan, al menos, en el plano indiciario". El TS también afirma que este principio "sirve para excluir la odiosa posibilidad de "rastreos" o exploraciones genéricas e indiscriminadas, predelictuales o de prospección, que supondrían un grave atentado contra el derecho al secreto de las comunicaciones de la generalidad de los ciudadanos, por ausencia de fundamento específico de la diligencia"[13] y que "en el caso de los descubrimientos ocasionales en estos supuestos en que se investiga un delito concreto y se descubre otro distinto, no puede renunciarse a investigar la *notitia criminis* incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello pueda hacer precisa una nueva o específica autorización judicial o una investigación diferente de la del punto de arranque".[14]

A continuación, voy a hacer referencia a otro de los principios por los que se rige esta materia, el principio de idoneidad, regulado también en el nuevo artículo 588 bis a, en este caso en el apartado 3, que establece que el principio de idoneidad "servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad".

En virtud de este artículo, la injerencia en el derecho derivada de la medida ha de ser adecuada u óptima para la consecución del fin que persigue. En otras palabras, para que la medida de investigación sea considerada idónea y, por lo tanto, acorde a este principio, la medida ha de ser capaz de conseguir el fin perseguido por la investigación en cuestión, es decir, debe servir objetivamente para la finalidad constitucionalmente legítima, proporcionando datos útiles para la investigación del delito.

---

[12] *Cfr*. SSTS 276/96 de 2 de abril,: ES:TS:1996:2030, 792/2007 de 30 de mayo, ES:TS:2007:6384, 457/2010 de 25 de mayo,: ES:TS:2010:2665, 426/2016 de 19 de mayo, ES:TS:2016:2149, 71/2017, de 8 de febrero, ES:TS:2017:441.

[13] *Cfr*: STS 985/2009, de 13 de octubre. ES: TS: 2009:6139. F.4.

[14] *Cfr*: STS 71/2017, de 8 de febrero. ES: TS: 2017:441. F.2.

El TS ha manifestado en varias de sus sentencias que una medida de investigación tecnológica resultará idónea cuando aparezca adecuada a los fines de la instrucción o cuando permita seguir avanzando con la misma.[15] En definitiva, este principio de idoneidad exige que la resolución judicial que acuerde la adopción de una de estas medidas deberá valorar la aptitud potencial para la obtención de resultados relevantes sobre el objeto y sujeto investigado y sobre la duración de la medida, es decir, exige que, "a la vista de las circunstancias del caso concreto, pueda hacerse pronóstico fiable de éxito, medido en la obtención de resultados útiles para la investigación del delito y su autoría".[16]

Para continuar con la exposición de los principios rectores, voy a analizar conjuntamente los principios de excepcionalidad y necesidad, puesto que así están regulados en la LECrim. Ambos están recogidos conjuntamente en el apartado 4 del artículo 588 bis a, que establece que, con base en estos principios,

> *"*solo podrá acordarse la medida cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida*"*.

Dada la redacción del artículo, podemos observar que ambos principios están íntimamente relacionados. Se pretende que la medida se considere necesaria para el caso concreto y que dicha medida no pueda ser reemplazada por otra que afecte en menor medida al derecho correspondiente y que sea igual de eficaz para el conocimiento del hecho y de su posible autor. En otras palabras: que la medida solo tenga lugar cuando no se encuentre otro instrumento distinto que permita los mismos resultados y que incida en menor medida en los derechos fundamentales del investigado.

En este sentido se ha pronunciado el TS, estableciendo que la adopción de una de estas medidas está justificada cuando no se alcance otra línea de investigación lícita[17], sin perjuicio de que estas medidas no son un medio normal de investigación sino que deben utilizarse de

---

[15] *Cfr*: STS 85/2017, de 15 de febrero, ES: TS: 2017: 476; STS 993/2016, de 12 de enero de 2017, ES: TS: 2017: 81; STS 982/2016, de 11 de enero de 2017, ES: TS: 2017: 40.

[16] ASENCIO MELLADO, José María. *Derecho procesal penal, op. cit.,* p. *235*.

[17] *Cfr*: STS 279/2017, de 19 de abril. ES: TS: 2017:1642. F.2.

manera excepcional no rutinaria puesto que no dejan de ser una limitación a un derecho fundamental[18].

Esta cuestión también ha sido objeto de regulación en el Convenio Europeo para la protección de los Derechos Humanos, concretamente en su artículo 8.2, y en la Carta de los Derechos fundamentales de la Unión Europea, en su artículo 52.1. En ambos casos se hace referencia a la exigencia de que se cumpla el principio de necesidad a la hora de adoptar estas medidas limitativas de derechos[19].

En síntesis, se requiere que la autorización judicial que habilite la medida de investigación justifique expresamente que dicha medida es necesaria para conseguir los resultados que se pretenden obtener y que estos no pueden lograrse mediante otras medidas que resulten menos lesivas para los derechos fundamentales del investigado, lo que convertiría esta medida en indispensable e insustituible para ese caso concreto.

Y por último en lo que a los principios rectores se refiere, cabe mencionar el principio de proporcionalidad, regulado en el apartado 5 del artículo 588 bis a LECrim, por el cual se establece que

> "las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

En virtud de este artículo, teorizamos que este principio es determinante a la hora de legitimar la medida de investigación tecnológica y su correspondiente injerencia en el derecho, requiere que la medida no suponga un sacrificio excesivo para la persona investigada, por lo que habrá que comprobar si el resultado que se pretende obtener con la adopción de esta medida resulta proporcionado en relación con la limitación al derecho fundamental afectado, atendiendo a la gravedad del hecho ilícito y a los indicios apreciados de su comisión.

---

[18] *Cfr*. STS 104/2011, de 1 de marzo. ES: TS: 2011:1316. F. 9.

[19] Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal (BOE n.º 70 de 22 de marzo de 2019).

Para comprobar si la medida se adecúa a este principio de proporcionalidad habrá que valorar, por un lado, los derechos e intereses que van a verse afectados por la medida y por otro, el interés público y de terceros. Con la nueva regulación se aumentan y se adaptan mejor a la realidad los criterios a tener en cuenta para realizar esta valoración del interés público. Estos criterios deberán aparecer en la resolución judicial habilitante, criterios que serán tanto cuantitativos como cualitativos, y con los que se comprobará si resulta legítima la adopción de la medida.

El primero de estos criterios viene constituido por la gravedad del hecho. Para atender a este criterio hay que tener en cuenta tanto la calificación de la pena legalmente prevista, como los bienes jurídicos protegidos y la relevancia. En este sentido, se ha reiterado desde hace años la jurisprudencia, como podemos observar en la STS 529/1996, 18 de Julio de 1996, en la que el Tribunal habla ya de la

> "necesidad de poner el acento no sólo en la gravedad de la pena fijada al presunto delito investigado sino también la transcendencia social del tipo, excluyéndose así cualquier autorización judicial en blanco, sin especificación delictiva, en tanto ello supondría la imposibilidad de valorar aquel juicio de equilibrio y ponderación".

En la misma línea jurisprudencial se ha pronunciado el TC, en sentencias posteriores, afirmando que "la gravedad de los hechos no ha de determinarse únicamente por la calificación de la pena legalmente prevista, sino que también han de tenerse en cuenta el bien jurídico protegido y la relevancia social de la actividad"[20].

Un ejemplo de la importancia de este criterio a la hora de determinar si la medida adoptada cumple con el principio de proporcionalidad lo podemos ver reflejado en la STS 985/2009, de 13 de octubre, cuando expresa que "la gravedad de los hechos investigados, posible integración en organización terrorista, no admite duda acerca de la proporcionalidad de la diligencia autorizada"[21].

Por otro lado, otro de los criterios a tener en cuenta a la hora de valorar la proporcionalidad de la medida, es la trascendencia social del hecho investigado o el ámbito tecnológico de producción, que podrá concurrir cumulativamente o no con el anterior criterio. Este criterio ha venido siendo admitido por la doctrina jurisprudencial desde hace

[20] *Cfr*: STC 14/2001, de 29 de enero, ES:TC:2001:14 Fj.3.

[21] *Cfr*: STS 985/2009, de 13 de octubre, ES:TS:2009:6139,Fj.3.

años, por ejemplo, en la STS nº 1241/2005, de 27 de octubre, se expresaba literalmente que "existe proporcionalidad de la medida porque la gravedad y trascendencia social del delito de tráfico de drogas justifica su adopción, y sacrificio del derecho al secreto de las comunicaciones"[22]. Asimismo, la STS 1898/2000, de 12 diciembre, en la que se cuestiona la interceptación de las comunicaciones telefónicas en un delito de revelación de secretos, en concreto, cuando en los fundamentos jurídicos se expresa que "dada la trascendencia social del ilícito investigado no cabe cuestionar en este caso la proporcionalidad entre la gravedad de la medida y la gravedad del hecho punible".

Y respecto al ámbito tecnológico de producción podemos decir que la razón estriba en el mayor alcance potencial del medio empleado, ya que muchos delitos son cometidos a través de la red y la práctica de estas diligencias es la única forma de llevar a cabo su investigación. En este sentido, se puede ver en la STC 104/2006, de 3 de abril, cuando el Tribunal habla "de la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito".[23]

Asimismo, otro de los criterios que tenemos que tener en cuenta es la intensidad de los indicios, que hace posible calibrar el nivel de desarrollo de la conducta delictiva y la participación del investigado, además de un análisis más ponderado sobre el grado de injerencia en el derecho.

Y por último en lo que se refiere a los criterios determinantes de la proporcionalidad, mencionar la relevancia del resultado perseguido, que engloba tanto la incidencia del descubrimiento como el efecto de la medida en el restablecimiento de la paz social perturbada por el delito.

Para finalizar con este principio de proporcionalidad, la jurisprudencia ha venido reiterando que para comprobar la proporcionalidad de la medida habrá que analizar las circunstancias concurrentes en el momento de su adopción[24].

En resumen, y a modo de concluir con el estudio de los principios rectores, es preciso reiterar que la concurrencia de estos principios "determina la legitimidad de la medida adoptada, desde el punto de vista constitucional, y "el respeto a los mismos garantiza que

---

[22] *Cfr*. STS nº 1241/2005, de 27 de octubre, ES:TS:2005:6544, Fj.1.

[23] *Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, op. cit.,* p. *12.*

[24] SSTC 14/2001, de 29 de enero, ES:TC:2001:14, Fj.2; 126/2000, de 16 de mayo, ES:TC:2000:126, FJ 8; 299/2000, de 11 de diciembre, ES:TC:2000:299, FJ 2.

tanto la medida como los resultados obtenidos serán prueba válida y lícita a efectos de la acusación o la defensa".[25]

3.1.3. Solicitud de la autorización judicial

La superación del correspondiente juicio de proporcionalidad lleva al juez encargado de la instrucción a autorizar, por auto, la práctica de la medida. Para ello, previamente, hay que hacer referencia al artículo 588 bis b LECrim, que regula la solicitud de dicha autorización judicial.

En el primer apartado de dicho artículo se establece que "el juez podrá acordar las medidas reguladas en este capítulo de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial". Con ello se deduce que están legitimados para solicitar la medida el Ministerio Fiscal y la Policía Judicial, incluyendo también dentro del ámbito de la Policía Judicial a las policías autonómicas como el Servicio de Vigilancia Aduanera. Además, también es posible que sea el Juez de Instrucción el que directamente la adopte de oficio.

Por otro lado, en el segundo apartado de este artículo se nos habla del contenido de dicha solicitud, que establece que:

> "Cuando el Ministerio Fiscal o la Policía Judicial soliciten del juez de instrucción una medida de investigación tecnológica, la petición habrá de contener: 1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos. 2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia. 3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida. 4.º La extensión de la medida con especificación de su contenido. 5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención. 6.º La forma de ejecución de la medida. 7.º La duración de la medida que se solicita. 8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse."

3.1.4. Resolución judicial

La medida de investigación tecnológica ha de ser autorizada o denegada por el juez de Instrucción, a través de auto motivado, previa audiencia del Ministerio Fiscal, y en un plazo

[25] MONTERO AROCA, *Juan. Derecho jurisdiccional III, op. cit.,* p. 246.

máximo de veinticuatro horas desde la presentación de la solicitud, como así lo establece el artículo 588 bis c, en su apartado primero.

Por otro lado, en su apartado segundo, se establece que, el juez, antes de resolver, y siempre que resulte necesario para el cumplimiento de los requisitos exigidos, y tanto materiales como formales, podrá requerir una ampliación o aclaración de los términos de la solicitud. En este caso se interrumpirá el plazo de las veinticuatro horas.

El apartado tercero por su parte establece cual ha de ser el contenido de la resolución judicial que autorice la medida, y expresa que dicha resolución concretará, al menos, los siguientes extremos[26]:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida
b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido
c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a
d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención
e) La duración de la medida
f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida
g) La finalidad perseguida con la medida
h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia

3.1.5. Requisitos y cuestiones de forma

La reforma de la LECrim ha considerado adecuado no abandonar los aspectos formales de la solicitud y del contenido de la resolución judicial habilitante. Las disposiciones comunes que integran este Capítulo IV se extienden igualmente a las demás cuestiones de forma, tales como la solicitud de prórroga, las reglas generales de duración, el secreto, el control de la

[26] *Vid.* art. 588 bis c), apartado 3º.

medida, la afectación a terceras personas, la utilización de información en procedimiento distinto, el cese de la medida o la destrucción de registros.[27]

En primer lugar, y siguiendo el orden fijado por la ley, el art. 588 bis d expresa que tanto la solicitud como las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa. Esto es así precisamente para preservar el resultado y éxito de la medida, puesto que si el sujeto tiene conocimiento de que se están usando cualquiera de estas medidas de investigación tecnológica contra él, es de imaginar que no dirá o hará nada que tenga relevancia penal en su contra. Por ello, se ha pensado que es necesario que toda solicitud de estas medidas lleve consigo la formación de una pieza separada y secreta.

Es preciso aclarar que el secreto solamente afectará a esa pieza separada, por lo que el resto del procedimiento sí se notificará al investigado. No obstante, el Fiscal valorará si es necesario instar el secreto de todo el procedimiento en los casos en los que el conocimiento del investigado pudiera llevar al fracaso de las medidas. Cada medida de investigación tecnológica que se tramite se hará en una pieza separada secreta, distinta y diferenciada, piezas que se abrirán con la solicitud de la medida de investigación. Estas piezas interrumpirán los plazos de duración de la fase de instrucción del procedimiento, puesto que, como establece el artículo 324 LECrim, en su apartado tercero, "los plazos previstos en este artículo quedarán interrumpidos en caso de acordarse el secreto de las actuaciones, durante la duración del mismo", y no se reanudarán hasta que no se alce el secreto para no perjudicar el derecho de defesa. En el mismo sentido, la Fiscalía General del Estado interpreta que "el secreto *ex lege* derivado de la adopción y ejecución de tales medidas de investigación, también generará el efecto de suspender el cómputo de los plazos del art. 324, al compartir la misma naturaleza y concurrir idéntico fundamento"[28].

En este orden de ideas, el artículo 588 bis e regula el tiempo de vigencia de la medida, y establece que estas medidas tendrán la duración que se especifique para cada una de ellas y que, en ningún caso, podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.

---

[27] Preámbulo IV. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

[28] Circular 5/2015, de 13 de noviembre, sobre los plazos máximos de la fase de instrucción.

La duración de cada medida de investigación tecnológica está afectada por tres límites: el primero, el plazo máximo de duración previsto por el legislador; en segundo lugar, ese plazo máximo deberá ser limitado por el juez en atención a las exigencias que los principios de idoneidad, necesidad, excepcionalidad y proporcionalidad presenten para el caso concreto; y en tercer lugar, la medida deberá cesar antes del plazo fijado si se hubiera logrado el esclarecimiento de los hechos o si se constatara que la diligencia no es adecuada para el fin que la justificó[29]. En el caso de que se sobrepase el plazo de intervención que se haya establecido, a partir de ese momento la información obtenida será considerada nula. La infracción de los plazos conlleva la nulidad de las realizadas fuera de plazo, pero en nada afectan a las tempestivamente obtenidas[30].

Además, en los apartados segundo y tercero de este mismo artículo se establece que la medida podrá ser prorrogada, mediante auto motivado, por el Juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron. Además, una vez transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos.

Por ende, es importante destacar que para que pueda tener lugar la prórroga de la medida es indispensable que subsistan las causas que lo motivaron.

La solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al Juez competente, con la antelación suficiente a la expiración del plazo concedido, como así dispone el artículo 588 bis f.

En concordancia con este artículo, la solicitud de prórroga deberá incluir necesariamente un informe detallado del resultado de la medida y las razones que justifiquen su continuación. El juez resolverá mediante auto motivado si procede a prorrogar la medida y lo hará en un plazo de dos días desde que se presente la solicitud, sin perjuicio de que antes pueda solicitar aclaraciones o mayor información si así lo considera necesario. La prórroga revestirá forma de auto y entrará a valorar si las causas y circunstancias que motivaron la resolución judicial habilitante continúan y justifican dicha prórroga.

En caso de acordar su prórroga, el plazo de esta comenzará a contarse desde la fecha de expiración del plazo de la medida acordada. Es decir, que aunque la prórroga se acuerde antes de su vencimiento, no por ello quedará acortado el plazo inicial fijado a la medida, y será cuando termine este plazo cuándo comenzará a contar el plazo de la prórroga.

---

[29] Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, *op. cit.*

[30] *Cfr*: STS 373/2016, de 3 de mayo, ES: TS: 2016:1942, F6.

Por otro lado, el acto de investigación está sujeto a otra de las cuestiones de forma a las que la ley hace mención, al control de la medida, recogido en el artículo 588 bis g, lo que conlleva a afirmar que la garantía de jurisdiccionalidad no solo afecta al acuerdo de la medida, sino que se extiende también al control de su desarrollo.

Literalmente, el artículo establece que la Policía Judicial informará al Juez de Instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que éste determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma. De ello deducimos que será el juez de instrucción el encargado de ejercer un control efectivo acerca de la intromisión en el derecho provocada por la medida. Para cumplir con lo dicho, la Policía judicial deberá informarle periódicamente sobre el desarrollo de la medida y sobre los resultados de esta, además de cualquier causa que ponga fin a la medida. Cuando finalice el procedimiento, es preciso que se eliminen los registros originales de los sistemas electrónicos o informáticos que hayan sido utilizados, y las copias de estos quedarán bajo custodia del LAJ durante 5 años, salvo que a juicio del Tribunal resulte precisa su conservación, como así establece el artículo 588 bis k).

En relación con lo anterior, hay que añadir que las medidas de investigación tecnológicas no solo afectan al investigado, sino que también pueden afectar a terceras personas ajenas a la investigación. Para que esto sea posible, se requiere que queden identificadas en la resolución judicial habilitante si fueran conocidos. En este sentido, el art. 588 bis h establece que podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Dentro de este capítulo de disposiciones comunes también se prevé la posibilidad de que, al llevar a cabo cualquiera de estas medidas de investigación tecnológicas, se descubra casualmente otra información relevante u otro delito diferente del que justificó la adopción de la medida. En este sentido, el artículo 588 bis i se remite al artículo 579 bis, y establece que el uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regula con arreglo a lo dispuesto en el artículo 579 bis. En relación con los "hallazgos casuales" es interesante destacar la Sentencia de "la manada de Pozoblanco", SJP de Córdoba 19/2020[31], en la que se cuestiona la validez de unas grabaciones encontradas al

[31] *Cfr*: SJP de Córdoba 19/2020, de 14 de abril,ES:JP:2020:19.

registrar, en el curso de otra investigación, los teléfonos de los investigados. Las grabaciones prueban la existencia de varios delitos cometidos por los acusados, entre otros, delitos de abusos sexuales. Los acusados, en su defensa, alegan la nulidad de dichas grabaciones por considerar que se ha tratado de una investigación de carácter prospectivo. El tribunal entiende que no se ha vulnerado ni el derecho al secreto de las comunicaciones ni el derecho a la intimidad de los investigados, por lo que rechaza la nulidad de las grabaciones, considerándolas como prueba plenamente lícita.

Siguiendo con la exposición del tema, el artículo 588 bis j se encarga de regular el cese de la medida. En él se establece que la vigencia de estas medidas queda sujeta a la regla *rebus sic stantibus* y que será el juez el que ha de acordar el cese de esta cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de esta no se están obteniendo los resultados pretendidos. El juez también cesará la medida cuando haya transcurrido el plazo para el que hubiera sido autorizada.

En último lugar, ha de hacerse alusión a la posibilidad de destrucción de los registros originales electrónicos cuando el investigado tenga interés legítimo en que no se conserven más allá de lo previsto en la ley. En efecto, el artículo 588 bis k establece que cuando se ponga fin al procedimiento mediante resolución firme, se borrarán los registros electrónicos que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, sin perjuicio de que el LAJ conserve una copia de estos durante 5 años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado. Transcurridos estos 5 años las copias se destruirán salvo que a juicio del Tribunal resulte precisa su conservación. De la destrucción de los registros se encargará la Policía Judicial bajo las órdenes oportunas que dicten los tribunales.

3.2. Interceptación de las comunicaciones telefónicas y telemáticas

3.2.1. Regulación y alcance de la medida

La primera de las diligencias de investigación tecnológica que regula la LECrim es la interceptación de las comunicaciones telefónicas y telemáticas, dedicando para ello los artículos 588 ter a a 588 ter m, correspondientes al Capítulo V del Título VIII del Libro II.

Esta diligencia consiste tanto en acceder al contenido de las comunicaciones telefónicas o telemáticas, como acceder al listado de llamadas realizadas o recibidas, o a los datos electrónicos de tráfico o asociados al proceso de comunicación, entendiendo por estos últimos "aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga", como dispone en su apartado segundo el artículo 588 ter b.

En consecuencia, nos encontramos efectivamente ante una diligencia de investigación limitativa del derecho al secreto de las comunicaciones, pero no en exclusiva, ya que por la naturaleza de muchos de estos datos a los que se va a poder acceder, no solo quedaría afectado el derecho al secreto de las comunicaciones, sino que podrían quedar afectados otros de los derechos previstos en el art. 18 CE, como el derecho a la intimidad o la protección de datos personales.

También hay que tener en cuenta que no todas las actuaciones derivadas de esta medida suponen la misma injerencia en los derechos del investigado. Es evidente que acceder al contenido de la comunicación supone una mayor incidencia en el derecho del investigado que acceder, por ejemplo, al listado de llamadas o a algunos de estos datos asociados. En este sentido ha expresado la jurisprudencia del TC que

> "aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las escuchas telefónicas, siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad"[32].

En el mismo sentido se han pronunciado Audiencias, como la Audiencia Provincial de Madrid, afirmando que "no cabe duda que la intervención telefónica y grabación de conversaciones supone una intromisión a la intimidad de los comunicantes superior a la intromisión que supone el simple recuento e identificación de las llamadas y de los números de teléfono utilizados desde el concreto teléfono objeto del recuento"[33]. En vista de lo

[32] *Cfr*: STC nº 26/2006, de 30 de enero, ES: TC: 2006: 26, FJ.7; STC 123/2002, de 20 de mayo, ES:TC:2002:123, FJ 6.

[33] SAP Madrid n.º 57/2002, de 4 de junio de 2002, ES:APM:2002:7155, Fj.1.5.3.3.

anterior, se tendrá que tener en cuenta el mayor o menos grado de injerencia a la hora de justificar la proporcionalidad de la medida.

La ley establece que los terminales o medios de comunicación telemática de los que sea titular o usuario el investigado son los que se van a poder intervenir, como así dispone el artículo 588 ter b, pero también se prevé la posibilidad intervenir los medios de comunicación de la víctima, siempre con finalidad protectora, cuando sea previsible un grave riesgo para su vida o integridad. En este sentido, podemos ver un ejemplo de la importancia que tiene esta posibilidad para la investigación de determinados delitos, en la SAP de A Coruña, el conocido caso de Diana Quer[34], en el que la intervención del móvil de la víctima fue crucial para la reconstrucción de los hechos, ayudando a conocer por donde se desplazó y a la velocidad a la que lo hizo, además del último mensaje de auxilio que mandó, logrando saber así que la víctima fue trasladada en un coche y que, además, estaba viva en el momento del traslado.

A pesar de esta regla general, también se contempla la posibilidad de que se intervengan terminales o medios de comunicación telemática de los que sea titular una tercera persona distinta del investigado. Para que se pueda dar esta posibilidad será necesario que exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad, como así dispone el artículo 588 ter c.
En definitiva, lo que se pretende con ello es evitar que se obstaculice la práctica de esta medida por el simple hecho de que el titular del terminal o del medio telemático no sea el propio investigado, cuando además, resulta bastante frecuente que el investigado no utilice sus propios medios de comunicación en la comisión del delito para así evitar ser descubierto. En este sentido podemos observar en la STS 441/2017, de 8 de febrero [35], entre otras, que la jurisprudencia ya admitía esta posibilidad desde hace años.

Además, el mismo artículo anterior también habla de otra situación que afectará a terceros cuando afirma que, "podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular", lo que se conoce coloquialmente como un hacker. Esta

[34] *Cfr*. SAP de A Coruña, ES:APC:2019:281.

[35] *Cfr*. STS 441/2017, de 8 de febrero, ES:TS:2017:441.

posibilidad "ya venía siendo admitida pacíficamente por nuestra doctrina jurisprudencial, como podemos observar en la STS n.º 1839/1994, de 18 de marzo"[36].

La práctica de esta diligencia ha sido muy frecuente desde hace muchos años, incluso antes de la reforma de la LECrimLECrim, siendo el objeto de muchas de las sentencias del TEDH, a las que me he referido *ut supra*[37], que alertaban de la necesidad de una ley que regulase de forma clara estas diligencias. En un primer momento, consistía básicamente en la interceptación de las comunicaciones telefónicas puesto que era la forma más habitual de comunicarse en ese momento. Hoy en día, habida cuenta de los grandísimos avances tecnológicos en este ámbito y el uso generalizado de internet, vemos como la medida alcanza también a medios telemáticos que podríamos calificar como "novedosos" y que se han vuelto imprescindibles a la hora de comunicarnos, como es el caso de la aplicación de mensajería *Whatsapp* o de las redes sociales. Un ejemplo de ello lo podemos encontrar en la STS 441/2017, de 8 de febrero, en la que aparece una referencia a un auto dictado en fase de instrucción en el que, expresamente, "se acuerda la observación, escucha y grabación tanto de conversaciones, como de mensajes de texto y de la aplicación "Whatsapp""[38].

A veces, en el curso de una investigación, lo que interesa no es la interceptación de las comunicación como tal, sino que lo que se necesita es, a través de una dirección IP, identificar el terminal o el dispositivo con el que se ha cometido el delito, para lo que el artículo 588 ter k establece que "se podrá requerir de los agentes sujetos al deber de colaboración, según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso".

Por otro lado, se prevé también la posibilidad de que la Policía Judicial pueda utilizar, sin necesidad de autorización judicial, ciertos artificios técnicos que permitan la identificación del terminal utilizado, accediendo a los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, como la numeración IMSI (identidad internacional del abonado móvil) o IMEI (identidad internacional del equipo

---

[36] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

[37] *Vid.* STEDH de 30 de julio de 1998, caso *Valenzuela Contreras c. España*, CE:ECHR:1998:0730JUD002767195

[38] *Cfr*: STS 441/2017, de 8 de febrero, ES:TS:2017:441.

móvil). Esta posibilidad se encuentra contemplada en el artículo 588 ter l apartado primero. Sin embargo, en el apartado segundo del mismo artículo, se establece que, una vez identificados los aparatos, se podrá proceder a la posterior intervención de las comunicaciones, para lo que sí será necesaria la correspondiente autorización judicial.

Finalmente, el artículo 588 ter m, regula la posibilidad de que, tanto el Ministerio Fiscal como la Policía Judicial, puedan dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, para conocer la titularidad de un número de teléfono o medio de comunicación o para conocer el número de teléfono o los datos identificativos de cualquier medio de comunicación. Los prestadores de servicios y el resto de los mencionados tendrán la obligación de prestar la información requerida, pudiendo incurrir de lo contrario en un delito de desobediencia.

3.2.2. Presupuestos, autorización y práctica de la medida

La ley delimita una serie de delitos para cuya investigación se permite la práctica de esta medida. Estos delitos están dispuestos en el artículo 588 ter a LECrim y son, en primer lugar, los delitos del artículo 579.1, es decir, los delitos dolosos castigados con una pena con límite máximo de al menos tres años de prisión, los delitos de terrorismo y los delitos cometidos en el seno de un grupo u organización criminal.

Respecto a los delitos dolosos castigados con una pena límite de al menos tres años de prisión, es preciso aclarar que se valorará con respecto a la pena en abstracto, sin tener en cuenta ni el grado de ejecución ni las posibles circunstancias modificativas de la responsabilidad criminal. Sobre esta cuestión cabe destacar la STJUE de 2 de octubre de 2018 que responde a una cuestión prejudicial planteada por la AP de Tarragona, acerca del umbral de los tres años de prisión. El Tribunal aclara que, como regla general, esta medida tiene lugar solo cuando estemos ante delitos graves puesto que "solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de grave", aunque admite también que "la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general sin que sea necesario que dichos delitos estén calificados como «graves»"[39].

[39] *Cfr*: STJUE de 2 de octubre de 2018, asunto C-207/16, EU:C:2018:788.

Además de los delitos a los que se refiere el artículo 579.1, la interceptación de las comunicaciones telefónicas y telemáticas también se permite en la investigación de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

En este caso, a la hora de justificar la proporcionalidad de la medida, hay que tener en cuenta que

> "los delitos cometidos a través de las nuevas tecnologías, difícilmente pueden investigarse a través de otros medios, y que la interceptación de las comunicaciones, y en particular las telemáticas, puede ser en ocasiones la única vía de investigación criminal de los ilícitos que se cometen a través de la red"[40].

Es preciso destacar que, el hecho de que se fijen una serie de delitos que permitan hacer uso de la medida, al igual que va a ocurrir con otras de las diligencias que explicaré posteriormente, no significa que se vaya a permitir su uso siempre que concurran los delitos mencionados, sino que también habrá que tener en cuenta los principios rectores que justifican dicha medida, regulados en el artículo ya mencionado 588 bis a[41], teniendo que "limitar el uso de la medida a la investigación de aquellos hechos que, por su especial gravedad, justifiquen la limitación de los derechos fundamentales"[42].

En otro orden de cosas, para poder llevar a cabo la interceptación de las comunicaciones telefónicas o telemáticas es necesaria una previa autorización judicial, que tendrá lugar en pieza separa y secreta para asegurar la efectividad de la medida.

La resolución judicial que habilite la medida tendrá forma de auto motivado y, en cumplimiento del artículo 588 ter d, deberá contener "la identificación del número de abonado, del terminal o de la etiqueta técnica, la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate".

---

[40] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

[41] Artículo 588 bis a. "Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida".

[42] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

Además de estas menciones, será necesario que, en virtud del mismo artículo, la resolución determine la extensión de la medida. Para ello, se ha de expresar si la medida consistirá bien en el registro o grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta, bien en el conocimiento de su origen o destino, en el momento en el que la comunicación se realiza, bien en la localización geográfica del origen o destino de la comunicación, o bien en el conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

En definitiva, para acordar la práctica de esta diligencia de investigación será necesaria, como norma general, la previa autorización judicial. No obstante, la ley permite una excepción para casos de urgencia en los que se permite que la medida sea acordada por el Ministerio del Interior o el Secretario de Estado de Seguridad, cuando haya razones fundadas que hagan imprescindible la práctica de la medida y siempre que nos encontremos en curso de investigación de delitos relacionados con bandas armadas o elementos terroristas. En estos casos, se tendrá que comunicar inmediatamente al juez, detallando la actuación realizada y las razones que la justificaron, en un plazo máximo de 24 horas, para que este ratifique o revoque la medida, en un plazo máximo de 72 horas desde que se ordenó la medida.

El artículo 588 ter e establece la obligación de determinadas personas de prestar al juez, al Ministerio Fiscal y Policía Judicial, la asistencia y colaboración precisas para facilitar el cumplimiento de la medida, pudiendo incurrir en un delito de desobediencia en caso de no hacerlo y, teniendo en todo caso, la obligación de guardar secreto acerca de estas actuaciones. Estas personas a las que se refiere el artículo son "los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual".

Una vez llevada a cabo la diligencia, la Policía Judicial deberá poner a disposición del juez, en los plazos establecidos y, necesariamente, en dos soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas, indicándose el origen y el destino de cada una de ellas. Además, el artículo 588 ter f, también señala que se han de adoptarse las medidas necesarias "mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable" para asegurar "la

autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas".

En principio, se establece una duración máxima de tres meses para la práctica de la medida, pero estos tres podrán ser prorrogados, mediante resolución judicial motivada, por periodos sucesivos de igual duración hasta un máximo de dieciocho, en virtud del artículo 588 ter g. Para solicitar la prórroga de la medida será necesario que se expresen las razones que justifiquen la necesidad de dicha prorroga, aportando la Policía Judicial "la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida"[43].

Para finalizar el análisis de esta medida, mencionar que, una vez que se dé por finalizada, las partes tendrán derecho a que se les entreguen las copias de las grabaciones y de las transcripciones realizadas, salvo aquellas que pudieran afectar a la vida íntima de las personas. Se requiere para ello el término de la vigencia de la medida y que se haya alzado el secreto, para evitar así que se interfiera el fin de la medida. También tendrán derecho a obtener la copia de éstas los terceros cuyas comunicaciones hayan resultado intervenidas.

Este derecho que tienen las partes a conocer que sus comunicaciones han sido intervenidas se encuentra regulado en el artículo 588 ter i, pero ya se venía admitiendo por el TEDH desde la sentencia de 6 de septiembre de 1978, caso *Klass y otros c. Alemania*, en la que se expresaba que 'Las medidas de vigilancia secreta deben ir acompañadas de garantías adecuadas y suficientes contra los abusos. Como estas medidas forzosamente impiden al interesado interponer un recurso efectivo, resulta indispensable que los procedimientos de control de las medidas que se instauren proporcionen las garantías apropiadas y equivalentes al recurso jurisdiccional, que protejan eficazmente los derechos del individuo"[44].

[43] Artículo 588 ter h LECrim.

[44] *Cfr*: STEDH de 6 de septiembre de 1978, *caso Klass y otros c. Alemania,* CE:ECHR:1978:0906JUD000502971.

3.3. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.

3.3.1. Regulación y alcance de la medida

La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos se encuentra actualmente regulada en el capítulo VI del Título VIII del Libro II de la LECrim, concretamente en los arts. 588 quater a, a 588 quater e.

Antes de la reforma de la LECrim, y la consiguiente introducción de estos artículos, se venía utilizando esta diligencia entendiéndola como una "modalidad de intervención de las comunicaciones amparada por el art. 579 de la Ley de Enjuiciamiento Criminal, únicamente sujeta a la correspondiente autorización judicial debidamente motivada"[45], como así se ha visto reflejado en numerosas sentencias del Tribunal Supremo[46]. El TEDH, por su parte, venía reiterando en sus sentencias que la captación y grabación de comunicaciones orales directas se encontraba dentro del ámbito del artículo 8 CEDH, y que por ello ha de estar siempre respaldada por una ley específica, ya que supone una intromisión en la vida privada del investigado. En este sentido, podemos observar la STEDH de 31 de mayo de 2005, *caso Vetter c. Francia,* donde se cuestionaba la vulneración del mencionado artículo 8 CEDH, por carecer de regulación sobre la materia en el momento de introducir los micrófonos en el interior del domicilio del investigado, a lo que el TEDH concluyó que "para proceder a la injerencia era necesaria la existencia de regulación legal sobre la materia, ya que están en juego derechos fundamentales y, por lo tanto, no se puede acudir a la aplicación analógica1"[47].

Con anterioridad a la reforma, ya el TC se manifestó, en su sentencia 145/2014, de 22 de septiembre, siguiendo la línea del TEDH. En dicha sentencia se cuestionaba la legitimidad de unas conversaciones verbales grabadas en las dependencias policiales por la posible vulneración derecho al secreto de las comunicaciones y de la intimidad, al no existir habilitación legal para llevarlas a cabo. El TC entendió que "la posibilidad de suplir los defectos de la ley, no puede ser trasladada a un escenario de injerencia en el secreto de las

[45] Circular 3/2019, de 6 de marzo, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.

[46] *Cfr.* SSTS nº 173/1998, de 10 de febrero,ES:TS:1998:853; 354/2003, de 13 de marzo, ES:TS:2003:1724; 419/2013, de 14 de mayo, ES:TS:2013:2450; 793/2013, de 28 de octubre, ES:TS:2013:5249.

[47] *Cfr. STEDH de 31 de mayo de 2005, caso Vetter c. Francia*, CE:ECHR:2005:0531JUD005984200.

comunicaciones en el que no exista previsión legal alguna"[48] y declaró la vulneración del art. 18.3 CE por la intervención de las comunicaciones verbales y la consiguiente nulidad de las grabaciones obtenidas. Esta sentencia sirvió como antecedente a la reforma, pero fue la propia LO 13/2015 la que finalmente dio el respaldo legal necesario a esta diligencia, para cumplir con las exigencias del CEDH.

Centrándonos ya en la explicación de esta medida, y atendiendo al art. 588 quater a LECrim y ss., podemos recalcar que esta diligencia consiste en la colocación de dispositivos electrónicos tanto en espacios abiertos y en vías públicas como en el domicilio del investigado u otros lugares cerrados, para acceder a las comunicaciones orales directas del investigado. Se hace referencia concretamente a las conversaciones orales directas, es decir, a las conversaciones que el investigado mantenga frente a frente con otra u otras personas, sin que se use para ello ningún aparato electrónico.

A diferencia de la diligencia anterior, aquí la comunicación "se capta por el dispositivo habilitado al efecto para recoger la imagen o sonido ambiente"[49], como puede ser un micrófono, una videocámara de vigilancia, o incluso el micrófono y la cámara del ordenador del investigado, mientras que en la interceptación de las comunicaciones, la comunicación se captaba a través del dispositivo telefónico o telemático.

Puesto que esta medida no solo se puede llevar a cabo en lugares abiertos, sino que también se pueden introducir estos dispositivos de grabación en el domicilio del investigado o en otros lugares cerrados destinados al ejercicio de la privacidad, no solo queda afectado el derecho al secreto de las comunicaciones, sino que también afecta al derecho a la privacidad y a la inviolabilidad del domicilio.

Por ello, en estos supuestos en los que sea necesario acceder al domicilio o a cualquier otro lugar destinado al ejercicio de la privacidad, el art. 588 quater a en su apartado segundo, obliga a que la resolución que autorice la medida extienda su motivación a la procedencia del acceso a estos lugares, de forma que quede justificada la limitación del derecho. Del mismo modo, en los supuestos en los que sea necesario colocar el dispositivo en un lugar en el que la persona investigada desarrolle su intimidad, como el dormitorio, "el auto deberá expresar

[48] *Cfr*: STC 145/2014, de 22 de septiembre,ES:TC:2014:145, Fj 7.

[49] Circular 3/2019, de 6 de marzo, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, *op. cit.*, p. 8.

las razones en las que se sostiene la necesidad de esta medida que deberá entenderse claramente excepcional"[50], reservándose este supuesto para casos especialmente graves.

Asimismo, esta medida podrá ser completada con la captación de imágenes cuando así se prevea en la resolución judicial, como así dispone el apartado tercero de este mismo artículo. También es preciso destacar que a la hora de colocar estos dispositivos de grabación en el interior del domicilio, y a pesar de que la medida vaya dirigida exclusivamente al investigado y no a terceros ajenos, es posible que también afecte a los derechos de otras personas distintas del investigado, como pueden ser sus familiares, por lo que no deja de ser una medida especialmente invasiva.

Hay que tener en cuenta que al captar o grabar las conversaciones del investigado no solo quedan afectados los derechos ya mencionados, sino que también cabe la posibilidad de que, en el transcurso de esas conversaciones, el investigado reconozca algún delito cometido con anterioridad, pudiendo quedar afectados el derecho a no confesarse culpable y a no declarar contra sí mismo, consignados en el artículo 24 CE.

En este sentido, el Tribunal Supremo afirma que

> "una cosa es almacenar en un archivo de sonido las conversaciones que pueden servir de prueba de la autoría de un hecho que se va a cometer o que se está cometiendo durante el desarrollo de la grabación y otra bien distinta es la grabación de un testimonio del que resulta la confesión de la autoría de un hecho ya perpetrado tiempo atrás. En el primero de los casos no se incorpora a la grabación el reconocimiento del hecho, sino las manifestaciones en que consiste el hecho mismo o que facilitan la prueba de su comisión. En el segundo, lo que existe es la aceptación de la propia autoría respecto del hecho delictivo ya cometido, lo que, en determinados casos, a la vista de las circunstancias que hayan presidido la grabación, podría generar puntos de fricción con el derecho a no confesarse culpable, con la consiguiente degradación de su significado como elemento de prueba y la reducción de su valor al de simple *notitia criminis,* necesitada de otras pruebas a lo largo del proceso"[51].

3.3.2. Presupuestos, autorización y práctica de la medida

A la hora de analizar los presupuestos hay que tener en cuenta que esta medida se prevé para un acto concreto de comunicación, es decir, un acto con carácter singular, puesto que

[50] ASENCIO MELLADO, José María. Derecho procesal penal, op. cit., p. 252.

[51] *Cfr*: STS n.º 517/2016, de 14 de junio, ES: TS: 2016: 2895, Fj.3.

la grabación ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad figuren indicios en investigación, como así establece el art. 588 quater b.

Para poder precisar el encuentro concreto y evitar que sea genérico, la Fiscalía General del Estado establece tres criterios de valoración. En primer lugar, habla de hacer una concreción locativa, es decir, se deberá precisar el lugar o dependencias y a los encuentros que van a ser investigados, como así lo establece el artículo 588 quater c, para evitar investigaciones prospectivas. En segundo lugar, será preciso hacer una concreción subjetiva y delimitar las personas que previsiblemente vayan a acudir al encuentro. Y por último, será necesaria una concreción temporal que delimite, en la medida de lo posible, el momento en el que va a tener lugar el encuentro o los encuentros, o en sus caso los indicios de este en caso de desconocerse la información exacta. Si bien es cierto que estos criterios ayudan a la concreción del encuentro, pero habrá que estar a las circunstancias de cada caso, puesto que a veces es suficiente con uno de ellos.[52]

Por otro lado, el artículo 588 quater b dispone que para que esta medida pueda ser adoptada es necesario, por un lado, que los hechos que estén siendo investigados sean constitutivos de ciertos delitos, en concreto, delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal o delitos de terrorismo.

Además, es necesario que se prevea racionalmente que el uso de esta medida aportará los datos relevantes para el esclarecimiento de los hechos y la identificación de su autor, lo que quiere decir que deberá incluirse una mención justificando la concurrencia de los principios de excepcionalidad y necesidad.

Respecto a la resolución judicial, el art. 588 quater c dispone que en ella se deberá precisar el lugar o dependencias y a los encuentros que van a ser investigados, además de la duración de la medida. Para grabar conversaciones en otros encuentros diferentes a los mencionados en la medida será necesario una nueva autorización judicial.

La resolución judicial deberá también precisar y fundamentar si lo que se está autorizando es la captación de las comunicaciones o la grabación de estas. Además, como ya

[52] Circular 3/2019, de 6 de marzo, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, *op. cit.*.

he mencionado, la autorización judicial puede extenderse también a la captación y grabación de imágenes.

Por otro lado, en virtud del art. 588 quater d, la Policía Judicial deberá poner a disposición de la autoridad judicial las grabaciones obtenidas con la medida y una transcripción de las conversaciones que se consideren relevantes. Además, se tendrá que identificar en el informe todos los agentes que hayan participado en la medida.

Respecto a la duración de la medida, el artículo 588 quater e simplemente se remite a lo ya dispuesto en el artículo 588 bis j, anteriormente analizado.

Finalmente, quiero hacer referencia a las grabaciones realizadas por particulares no autorizadas ni dirigidas por las autoridades judiciales. En estos casos, no se podrá valorar de la misma forma que si se hubiese realizado por la policía. Los jueces tendrán que realizar el correspondiente juicio de pertinencia respecto a los datos y circunstancias contenidos en el vídeo, y valorar "si concurre un fin legítimo que justifique la utilización en el proceso penal de esas imágenes y si su incorporación al proceso como prueba viene autorizada por los principios de necesidad, racionalidad y proporcionalidad"[53].

3.4. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

3.4.1. Regulación

La utilización de dispositivos técnicos de captación de la imagen, seguimiento y de localización es otra de las diligencias de investigación que encontramos regulada en la LECrim, concretamente en el Capítulo VII, del Título VIII del Libro II, correspondiente con los artículos 588 quinquies a a art. 588 quinquies c.

Se trata de medidas de investigación que consisten, por un lado, en la captación de imágenes de la persona investigada cuando se encuentre en un lugar público, y por otro, en la utilización de dispositivos de seguimiento y de localización, como así los diferencia la propia LECrim. En consecuencia, el artículo 588 quinquies a se refiere a la captación de imágenes en lugares públicos, estableciendo que

> "la Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos",

[53] *Cfr*: STS nº 793/2013, de 28 de octubre, FJ.2, ECLI: ES: TS: 2013: 5249.

y es el artículo 588 quinquies b el que dispone que "cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización". Para llevar a cabo esta medida, la Policía Judicial hará uso de medios técnicos como puede ser, la utilización de cámaras callejeras de video vigilancia, dispositivos GPS o balizas de seguimiento, o incluso hacer uso de otros medios más modernos y posiblemente más eficaces, como la localización GSM, "un servicio proporcionado por las empresas de telecomunicaciones que permite determinar la posición aproximada de un teléfono móvil gracias a su constante conexión con las estaciones BTS"[54].

3.4.2. La captación de imágenes

En primer lugar, voy a referirme a la captación de imágenes. A diferencia del resto de medidas de investigación, la grabación de la imagen en espacio público no necesita autorización judicial "en la medida en que no se produce afectación a ninguno de los derechos fundamentales del artículo 18 de nuestro texto constitucional"[55], sino que será la Policía Judicial la que se encargue de la práctica de esta medida, valorando posteriormente el Juez la concurrencia de los principios rectores en el caso concreto.

Por lo tanto, solo será necesaria la autorización judicial cuando se trate del domicilio del investigado o de otros lugares cerrados, es decir, cuando se trate de un lugar protegido por el derecho a la intimidad o a la inviolabilidad del domicilio. En este sentido, la jurisprudencia ha venido reiterando que será "legítima y no vulneradora de derechos fundamentales la filmación de escenas presuntamente delictivas que suceden en espacios o vías públicas"[56], entendiendo el carácter público desde la perspectiva de la privacidad y del ejercicio del derecho a la intimidad y no desde la titularidad.

De forma que, para saber si será necesaria la autorización, lo relevante será "discernir cuando se trata de un espacio reservado a la autorización judicial, domicilio o lugar cerrado, o cuando por propia iniciativa los agentes pueden captar las imágenes cuestionadas por tratarse de "lugares o espacios públicos""[57]. En relación con lo anterior, lo que si se requiere

---

[54] Circular 4/2019 de la FGE, de 6 de marzo, *sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.*

[55] Preámbulo IV. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

[56] *Cfr*: SSTS n.º 968/1998, de 17 julio,ES:TS:1998:4822; 67/2014, de 28 enero, ES:TS:2014:558; 409/2014, de 21 de mayo, ES:TS:2014:2209; 200/2017, de 27 de marzo,ES:TS:2017:1069.

[57] *Cfr*: STS n.º 272/2017, de 18 de abril, ES: TS: 2017: 1594. Fj 3.

es que "las condiciones de captación de las imágenes sean respetuosas con los derechos fundamentales de los afectados, en especial con el de la intimidad, de manera que no afecten a entornos o a espacios de privacidad"[58].

Con la captación de imágenes a través de cámaras de videovigilancia, es posible que también quede afectado el derecho a la protección de datos ya que "la imagen se considera un dato de carácter personal"[59], por lo que, para se consideren legítimas estas grabaciones y se pueda hacer uso de ellas como prueba en el proceso, será necesario que se ajusten a la Ley de Protección de Datos Personales y garantía de los derechos digitales y legislación complementaria. En este sentido podemos observar la STC n.º 39/2016, de 3 de marzo, en la que se cuestiona la vulneración de los derechos a la intimidad y a la protección de datos, al haber sido despedida la empleada como consecuencia de los datos obtenidos por la instalación de cámaras de videovigilancia. En este caso, el tribunal entiende que no se vulnera el derecho a la protección de datos por haber sido avisada la trabajadora de la instalación de dichas cámaras y porque las imágenes han sido utilizadas para el control de la relación laboral. Tampoco estima que haya vulneración de la intimidad dado que era una medida justificada, idónea para la finalidad de la empresa, necesaria y equilibrada.

Por otro lado, esta diligencia de investigación también puede afectar a otras personas distintas de la persona del investigado si fuese necesario para preservar la utilidad de la medida o si existen motivos fundados de que esas personas tienen relación con el investigado y con los hechos correspondientes, como así lo establece el artículo 588 quinquies a en su apartado segundo.

Finalmente, hay que mencionar que esta medida se deriva la posibilidad de que la policía haga uso de dispositivos que potencien la capacidad normal de observación, como drones, para grabar el interior del domicilio, grabando lógicamente desde un lugar público. En estos casos, al hacerse uso de estos dispositivos para la observación sí será necesaria una autorización judicial expresa, salvo que haya consentimiento de la persona interesada. En este sentido sobre la captación de imágenes por la Policía desde la vía pública, se ha

---

[58] *Cfr*: STSJ Cataluña 11/2011, de 5 de mayo, ES: TSJCAT: 2011: 5794; SSTS 157/1999 de 30 enero, ES:TS:1999:503; 968/1998 de 17 julio, ES:TS:1998:4822; 223/1998 de 3 septiembre, ES:TS:1998:5067; 1733/2002 de 14 de octubre, ES:TS:2002:6716; 299/2006 de 17 de marzo, ES:TS:2006:1517; 597/2010 de 2 de junio, ES:TS:2010:3136; 1140/2010 de 29 de diciembre, ES:TS:2010:7184.

[59] *Cfr*: STC n.º 39/2016, de 3 de marzo, ES: TC: 2016: 39. Fj 3.

pronunciado el TS en varias sentencias como la n.º 329/2016, de 20 de abril y la n.º 354/2003, de 13 de marzo, expresando que

> "el Estado no puede adentrarse sin autorización judicial en el espacio de exclusión que cada ciudadano dibuja frente a terceros. Y se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un utensilio óptico que permite ampliar las imágenes y salvar la distancia entre el observante y lo observado"[60]. En el este caso de esta primera sentencia, se cuestiona la validez de las observaciones de los agentes al interior del domicilio, sin ningún tipo de autorización y mediante la utilización de unos prismáticos. El Tribunal entiende que al hacer uso de los prismáticos, los agentes están observando más allá de lo que está a la vista de cualquiera y que por lo tanto se estarían vulnerando los derechos fundamentales de los investigados.
>
> En la segunda de las sentencias mencionadas, el Tribunal también precisa que "no estarían autorizados, sin el oportuno placet judicial, aquellos medios de captación de la imagen o del sonido que filmaran escenas en el interior del domicilio prevaliéndose de los adelantos y posibilidades técnicos de estos aparatos grabadores, aun cuando la captación tuviera lugar desde emplazamientos alejados del recinto domiciliario"[61].

3.4.3. La utilización de dispositivos o medios técnicos de seguimiento y localización

Respecto a la utilización de dispositivos o medios técnicos de seguimiento y localización ha quedado claro que, aunque de forma diferente, también afecta a derecho a la intimidad de la persona investigada, puesto que al conocer la información sobre los lugares a los que acude se puede a acceder a muchos datos sobre su vida privada, por ejemplo, la asistencia a un determinado templo religioso o simplemente el hecho de conocer los hábitos de una persona. A diferencia del caso anterior, hay que destacar que aquí sí que será necesaria la autorización judicial, como así lo dispone el art.588 quinquies b. La autorización se exige para la instalación y utilización de estos dispositivos. Distinto sería el caso del seguimiento físico por parte de los agentes de la policía, supuesto para el que no se requiere autorización.

La exigencia de autorización judicial para esta medida es una de las novedades introducidas por la reforma de la LECrim, puesto que la línea jurisprudencial anterior consideraba que la colocación de GPS o balizas de seguimiento por la Policía Judicial no afectaba a ningún derecho fundamental y que, por lo tanto, no era necesaria la previa

[60] *Cfr*: STS 329/2016, 20 de abril de 2016, ES: TS: 2016: 1709, Fj 2.

[61] *Cfr*: STS 354/2003, 13 de marzo de 2003, ES:TS:2003:1724, FJ,2.

autorización judicial. Ejemplo de ello lo podemos encontrar en las SSTS 523/2008, de 11 de julio, STS 906/2008, de 19 de diciembre y STS 798/2013, de 5 de noviembre[62].

A partir de la reforma, la línea jurisprudencial ha cambiado para adecuarse a la nueva legislación, y como afirma el TS

> "resulta pues evidente que, a partir de la entrada en vigor de la mencionada reforma de la Ley de Enjuiciamiento Criminal, la policía judicial española necesita autorización judicial para la utilización de dispositivos o medios técnicos se seguimiento o localización cuando puede resultar afectado el derecho a la intimidad de una persona"[63].

No obstante, a pesar de la exigencia de autorización judicial que habilite la medida, la ley prevé, en el apartado cuarto del artículo 588 quinquies b, que, excepcionalmente, cuando concurran razones de urgencia, y para evitar frustrar el fin de la medida, la Policía judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, que podrá ratificar la medida o cesar la medida en el mismo plazo.

El TEDH por su parte, no se paró a analizar de forma directa esta materia hasta el conocido *caso Uzun c. Alemania*, de 2 de septiembre de 2010[64], en la que manifestó que la vigilancia mediante dispositivos GPS constituía una injerencia en la vida privada, incluida en el ámbito del artículo 8 CEDH, pero que

> "por su propia naturaleza, debe distinguirse de otros métodos de seguimiento acústico o visual que, por regla general, son más susceptibles de interferir en el derecho de la persona al respeto de su vida privada porque revelan unas informaciones sobre la conducta de una persona, sus operaciones o sus sentimientos". El TEDH "estableció como criterio de especial relevancia, a la hora de dar protección a ese derecho a la vida privada que recoge el art. 8.1 del CEDH, el concepto de expectativa razonable de privacidad que ya manejó la sentencia del caso Katz"[65] contra Estados Unidos, 389 US 347.

---

[62] *Cfr*. SSTS 523/2008, de 11 de julio, ES:TS:2008:4616; 906/2008, de 19 de diciembre, ES:TS:2008:7266; 798/2013, de 5 de noviembre, ES:TS:2013:5313.

[63] *Cfr*: STS nº 610/2016, de 7 de julio, ES: TS: 2016: 3621, Fj 1.

[64] STEDH caso *Uzun c. Alemania,* de 2 de septiembre de 2010, CE:ECHR:2010:0902JUD003562305.

[65] *Cfr*: STS nº 610/2016, de 7 de julio, ES: TS: 2016: 3621, Fj 1.

Otro de los requisitos que prevé la ley es que la resolución judicial que habilite la medida especifique el medio técnico que se va a utilizar para llevarla a cabo, como así establece el artículo 588 quinquies b, en su apartado segundo.

3.4.4. Presupuestos y práctica de la medida

En este caso a diferencia de las diligencias anteriores, la ley no establece una serie de delitos para los que se pueda adoptar esta medida, pero sí añade un tercer artículo a este capítulo referido a su duración, el artículo 588 quinquies c. Con base en dicho artículo, la duración de esta medida no debe superar los tres meses, aunque se admite excepcionalmente su prórroga hasta un límite máximo de 18 meses, por supuesto motivando las razones excepcionales, y los medios a utilizar.

Cuando el seguimiento o localización se realice a través de la localización GSM se precisará, para el desarrollo de la medida, la colaboración de los prestadores de servicios de telecomunicaciones o de servicios de la sociedad de la información y de personas que contribuyan a facilitar la comunicación a través del teléfono o de otros medios o sistemas de comunicación telemática. Estas personas estarán obligadas a prestar al juez, al Ministerio Fiscal y Policía Judicial, la asistencia y colaboración precisas para facilitar el cumplimiento de la medida, como así establece el artículo 588 quinquies b en su apartado tercero, pudiendo incurrir en un delito de desobediencia en caso de no hacerlo.

En virtud del artículo 588 quinquies c, apartado segundo, será obligatoria la entrega al juez, por parte de la Policía Judicial, de los soportes originales o copias electrónicas auténticas que contengan la información recogida, en cualquier momento en que el juez así lo solicite y, en todo caso, una vez finalizada la medida. En el caso de que se trate de datos electrónicos asociados a sistemas de comunicación telefónica "serán las compañías prestadoras de servicios de telecomunicación las que habrán de remitir tales datos, cuya autenticidad quedará garantizada por medio de los protocolos que se encuentran implementados en los sistemas empleados para la recepción de tales datos"[66], como SITEL[67].

[66] Circular 4/2019, de 6 de marzo, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, *op. cit.*

[67] SITEL: sistema para interceptar y recopilar comunicaciones telefónicas y telemáticas, perteneciente al Ministerio de Interior de España, y al que tienen acceso tanto el CNI como los cuerpos y fuerzas de seguridad del Estado.

Y para terminar, añadir que la información obtenida a través de los dispositivos técnicos de seguimiento y localización deberá ser debidamente custodiada para evitar su utilización indebida, como así establece el apartado tercero del artículo antes mencionado.

3.5. Registro de dispositivos de almacenamiento masivo de información

3.5.1. Regulación y alcance de la medida

El registro de dispositivos de almacenamiento masivo de información se encuentra regulado en el capítulo VIII, del mismo título al que nos hemos venido refiriendo, concretamente en los artículos 588 sexies a a 588 sexies c.

Esta medida de investigación consiste en el acceso, y el registro posterior, de dispositivos de almacenamiento masivo de información, como puede ser un USB o un disco duro. Dentro del concepto de dispositivos de almacenamiento masivo de información se comprenden "no solo los instrumentos capaces de grabar, almacenar y posteriormente recuperar o leer información digital, sino también los soportes empleados para ello y que carecen de funcionalidad sin el dispositivo que en ellos escribe o lee"[68].

Dada la importancia que ha ido adquiriendo la tecnología en nuestras vidas, este tipo de dispositivos pueden guardar una cantidad inmensa de datos sobre la vida de la persona, por lo que, con su registro pueden quedar afectados varios derechos de la persona investigada. Así, el TC expresaba en la sentencia 173/2011, 7 de noviembre, que

> "si no hay duda de que los datos personales relativos a una persona individualmente considerados, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano". A esto añadía que "cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud,

[68] Circular 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos.

orientaciones sexuales, etc". El Tribunal afirmaba que quizá estos datos analizándolos individualmente carecían de relevancia, pero que analizándolos en su conjunto "no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular"[69].

El acceso a estos dispositivos de almacenamiento masivo de información puede afectar no solo al derecho a la intimidad del investigado, por las razones a las que me acabo de referir, sino que también es posible la afectación al derecho al secreto de las comunicaciones, ya que, a la hora de registrar un dispositivo como puede ser un ordenador, por ejemplo, que se trata también de un "instrumento útil para la emisión o recepción de correos electrónicos"[70], también queda afectado este derecho.

La línea jurisprudencial anterior venía haciendo esta diferencia y, de hecho, la exigencia o no de autorización judicial dependía del derecho que quedara afectado con la medida[71], pero actualmente, se viene entendiendo que en un dispositivo informático podemos encontrar una gran variedad de datos de distinta naturaleza, que van a ser entendidos de forma unitaria, dando lugar a un nuevo concepto que abarca a todos ellos, el derecho al entorno virtual, siendo ahora irrelevante distinguir si queda afectado uno u otro derecho.

En este sentido, el TS justifica el tratamiento unitario afirmando que

"la consideración de cada uno de estos datos de forma separada y con un régimen de protección diferenciado es insuficiente para garantizar una protección eficaz, pues resulta muy difícil asegurar que una vez permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad (por ejemplo, los contactos incluidos en la agenda), no se pueda acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo"[72]. Por ello, se precisa que "la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel

[69] *Cfr*. STC 173/2011, 7 de noviembre, ES: TC: 2011: 173, Fj 3.

[70] Ibidem

[71] *Vid*. STC n.º 230/2007, de 5 de noviembre, ES:TC:2007:230; STC n.º 115/2013, de 9 de mayo, ES:TC:2013:115.

[72] *Cfr*. STS 204/2016, 10 de marzo de 2016, ES: TS: 2016: 1218, Fj 11.

dispositivo"[73], porque "más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual"[74].

Es común que esta diligencia se practique junto con la entrada en el domicilio del investigado o en un lugar cerrado, puesto que, una vez dentro de estos lugares, será necesaria también la autorización judicial para poder acceder a la información de los dispositivos encontrados en el interior de estos. En este sentido se ha pronunciado el TS, afirmando que "la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados"[75]. Por ello, el artículo 588 sexies a, dispone que:

> "cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos".

En el caso de que estos dispositivos sean encontrados de forma diferente o en otro tipo de lugares, se deberá poner en conocimiento del juez para la correspondiente autorización, cumpliendo así con la exigencia del artículo 588 sexies b.

3.5.2. Presupuestos y autorización

El acceso al contenido de estos dispositivos necesita de una autorización que lo permita, salvo en casos en que concurran razones de urgencia y resulte imprescindible llevar a cabo esta medida. Como ya he mencionado anteriormente, cuando me refería a los derechos que quedan afectados por la medida, la línea jurisprudencial anterior a la reforma solo exigía la existencia de dicha autorización judicial cuando la práctica de la medida afectaba al secreto de las comunicaciones. Esta exigencia ha cambiado a raíz de la reforma, siendo ahora necesaria la autorización judicial para llevar a cabo esta diligencia de investigación, cumpliendo así con las exigencias del TEDH, que ya había declarado en la sentencia de 22

---

[73] *Cfr*. STS nº 342/2013, de 17 de abril, ES: TS: 2013: 2222, Fj 8; STS nº 786/2015, de 4 de diciembre, ES: TS: 2015: 5362., Fj 1.

[74] Ibidem.

[75] Cfr. STS nº 342/2013, de 17 de abril, ES: TS: 2013: 2222, Fj 8.

de mayo de 2008, *caso Iliya Stefanov c. Bulgaria*[76], y por "el Tribunal Supremo de Estados Unidos que, en su sentencia de 25 de junio de 2014 (casos acumulados Riley contra California y Estados Unidos contra Brima Wurie -573 U.S.- 2014), destacaba la gravísima afectación de la privacidad que podía derivarse de un examen indiscriminado y sin límites de un teléfono inteligente"[77].

La resolución por la que se autorice la medida tendrá también forma de auto y deberá cumplir con las exigencias establecidas en el artículo 588 sexies c, apartado primero, teniendo que fijar el alcance de dicha medida, las condiciones necesarias para asegurar la integridad de la información, y limitar la medida en lo posible a la realización de copias de los datos hallados para evitar la incautación de los dispositivos. En otras palabras, lo que se pretende es delimitar los dispositivos que se van a poder registrar y la naturaleza de los datos que van a poder registrarse.

El artículo 588 sexies c, en su apartado tercero, permite la ampliación del registro por el juez cuando se tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. En caso de urgencia se faculta a la Policía Judicial o al fiscal para llevar a cabo esta ampliación del registro, teniendo por supuesto que informar inmediatamente al juez en un plazo máximo de 24 horas, y teniendo este que ratificarlo o revocarlo en 72 horas desde que fue ordenada la medida.

El registro de dispositivos de almacenamiento masivo de información requiere para ello la correspondiente autorización, salvo en casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida. En estos supuestos, el apartado cuarto de este artículo 588 sexies c, habilita a la Policía Judicial para que pueda directamente llevar a cabo la diligencia siempre que así se le comunique al juez, por escrito y en un plazo de 24 horas para que el ratifique o cese la medida en un plazo, en este caso, no superior a 72 horas desde que fuera ordenada su práctica.

En este sentido, tanto la doctrina del TS como del TC expresan que "ha de asegurarse que la invasión policial directa tenga un carácter excepcional, y solo puede justificarse, en

[76] STEDH de 22 de mayo de 2008, caso Iliya Stefanov c. Bulgaria, CE:ECHR:2008:0522JUD006575501.

[77] Circular 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos, op. cit..

casos de urgencia y necesidad, que hagan imprescindible la medida"[78], y que "han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad"[79].

Para concluir, los agentes de la policía podrán requerir colaboración de toda persona que conozca el funcionamiento de dichos dispositivos para facilitar la información necesaria, en virtud del apartado 5 del mismo artículo 588 sexies c, pudiendo incurrir en un delito de desobediencia si no lo hacen, salvo el propio investigado o las personas que se encuentren exentas del deber de declarar ya sea por razones de parentesco o por cumplimiento del secreto profesional.

3.6. Registros remotos sobre equipos informáticos

3.6.1. Regulación y alcance de la medida

La LECrim regula en el Capítulo IX, del mismo Título VIII, la última diligencia de investigación tecnológica, el registro remoto sobre equipos informáticos. A su desarrollo dedica los artículos 588 septies a a 588 septies c.

Esta medida de investigación consiste en la utilización a distancia, desde centros de control policial, de un software o programa informático que permita conocer el contenido de los dispositivos electrónicos del investigado, pero sin tener que acceder materialmente a ellos. Coloquialmente se conoce esta técnica como "gusano informático" o "troyanos buenos" y con ella se accede a todos los datos incluidos en estos dispositivos sin distinción alguna. En estos tiempos en los que la sociedad está tan digitalizada, es muy probable que estos dispositivos contengan información sobre muchos aspectos de la vida privada del investigado, por lo que al acceder al contenido de estos, igual que ocurría con la diligencia de investigación analizada anteriormente, se accede también a contenido sobre la vida privada, quedando afectados en gran medida todos los derechos del art 18 CE, incluido también el derecho a la protección de datos.

A diferencia del registro de dispositivos de almacenamiento masivo de información, esta diligencia se va a llevar a cabo sin el conocimiento del investigado y además, va a tener carácter dinámico, puesto que se van a conocer todos los datos que se encuentren en el dispositivo a lo largo de la medida, es decir, los que se vayan añadiendo y los que se vayan

[78] *Cfr*: STS nº 204/2016, de 10 de marzo, ES: TS: 2016: 1218, FJ15.

[79] *Cfr*: STC 206/2007, de 24 de septiembre, ES: TC: 2007: 206, FJ 8; STS 864/2015, de 10 de diciembre, ES: TS: 2015: 5809.

borrando hasta que finalice la medida, por lo que podríamos decir que se trata de una diligencia de investigación más invasiva que la anterior y por lo tanto, con mayores limitaciones.

Esta medida, igual que ocurría con la anterior, permite tener acceso al entorno virtual del investigado, es decir, a todos los datos que se puedan encontrar en el interior del dispositivo intervenido, aunque esto afecte también al derecho al secreto de las comunicaciones. Pero no es solo eso, sino que además, y dado el carácter dinámico de esta medida, no solo se tendrá acceso a las comunicaciones existentes en el momento del registro, sino que abarcará todas las conversaciones desde el inicio hasta el fin de la medida, por lo que podemos decir que esta diligencia de investigación se encuentra a medio camino entre el registro de dispositivos de almacenamiento masivo de información y la interceptación de las comunicaciones telemáticas.

3.6.2. Presupuestos, autorización y práctica de la medida

Para llevar a cabo esta diligencia de investigación, la ley prevé en el artículo 588 septies a, en su apartado primero, tanto la utilización de datos de identificación y códigos, utilizando las propias contraseñas del investigado, como la instalación de un software, con la finalidad en ambos casos de examinar a distancia el dispositivo del investigado, de forma remota y telemática y sin su conocimiento. El segundo de los casos, la diligencia suele consistir en utilizar programas que permitan acceder a los dispositivos del investigado, como "troyanos" o "keylogger", y que quizá resulte más complicado debido a que el investigado puede tener protegido el dispositivo, dificultando así el acceso a ellos.

Es curioso que "España es uno de los pocos países de la Unión Europea que regula expresamente el registro remoto de equipos informáticos a través de la instalación de software espía como una medida de investigación criminal"[80], Francia e Italia, por ejemplo, también regulan esta medida como diligencia de investigación.

Puesto que el registro remoto sobre equipos informáticos se trata de una medida extremadamente invasiva para los derechos del investigado, se establecen una serie de exigencias extra para su adopción. En primer lugar, se establece un *numerus clausus* de delitos para los que se podrá utilizar esta diligencia. Así, el apartado primero del artículo 588 septies a, establece que solo podrá ser adoptada esta medida cuando la investigación verse sobre delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos

80. BACHMAIER WINTER, Lorena. "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015". *Boletín del Ministerio de Justicia*, año 71, n. º 2195, 2017, p.7.

cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional, y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. En relación con estos últimos, es preciso destacar que, a pesar de establecer la ley un *numerus clausus* de delitos, se trata de una previsión que puede ser muy amplia y que, además, la ley tampoco establece un mínimo de pena, por lo habrá que tener especialmente cuidado a la hora de valorar el cumplimiento del principio de proporcionalidad[81].

Otro de los requisitos que exige la ley para poder llevar a cabo esta medida de investigación es que sea acordada por el juez, y además establece los requisitos que ha de cumplir esta resolución judicial.

La resolución judicial será un auto debidamente motivado que, con base en lo dispuesto en el apartado segundo del artículo anteriormente mencionado, "deberá especificar:

> a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.
>
> b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
>
> c) Los agentes autorizados para la ejecución de la medida.
>
> d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
>
> e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso."

En virtud del apartado tercero de este mismo artículo, el juez podrá acordar la ampliación de esta medida a otros dispositivos del investigado cuando haya razones fundadas de que los datos buscados se encuentran en ellos.

La Policía Judicial será quien se encargue de la práctica de la medida, sirviéndose para ello de la colaboración de los prestadores de estos servicios, de los titulares y responsables del sistema informático o bases de datos objeto de registro, y, en definitiva, de cualquier

[81] Ibidem.

persona que conozca el funcionamiento de los dispositivos para proteger el fin de la medida. Estas personas están obligadas a prestar la colaboración en base al artículo 588 septies b, para lograr el buen fin de la diligencia, salvo, evidentemente, el investigado y las personas exentas del deber de declarar por razones de parentesco o secreto profesional.

En cuanto a su duración, la ley establece que el registro remoto de dispositivos electrónicos tendrá una duración máxima de un mes, que podrá prorrogarse por periodos iguales hasta un máximo de tres meses, como así dispone el artículo 588 septies c. Como podemos observar, los plazos que dispone la ley para la práctica de esta medida, son bastante inferiores con respecto a los establecidos para el resto de las medidas, lo que se fundamenta en lo especialmente invasiva que resulta esta medida.

3.7. El agente encubierto informático

Para finalizar la presente exposición, quiero hacer referencia a la figura del agente encubierto[82], más concretamente al agente encubierto informático[83].

Esta figura ha sido introducida en la LECrim con la LO 13/2015, que añadió al artículo 282 bis LECrim los apartados 6 y 7, creando así la figura del agente encubierto informático. Desde ese momento se regula esta figura como una diligencia más de investigación, que seguirá prácticamente las condiciones fijadas para el agente encubierto tradicional.
Se trata de una medida de investigación utilizada en la investigación de delitos cometidos por organizaciones criminales, que permite a los agentes de la Policía Judicial infiltrarse y actuar en la red, introduciéndose en canales cerrados de comunicación, utilizando para ello una identidad supuesta, ocultando evidentemente su identidad policial, y con el fin de esclarecer los hechos delictivos.

La doctrina distingue "lo que se conoce como ciber patrulleo (el agente realiza exploraciones o indagaciones por canales abiertos de comunicación) y el estricto agente encubierto online que opera en canales cerrados"[84], incluyéndose solamente dentro del

---

[82] Sobre la figura del agente encubierto, se recomienda la lectura siguiente: GASCÓN INCHAUSTI, Fernando. *Infiltración policial y "agente encubierto"*. Comares: Granada, 2001.

[83] SÁNCHEZ GÓMEZ, Raúl. "*La Ley Penal*" n.º 118, Sección Estudios, Enero-Febrero 2016, Editorial LA LEY. Disponible en: https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiNjAxMzU7Wy1KLizPw8WyMDQzMDIyOwQGZapUt-ckhlQaptWmJOcSoAMId3nzUAAAA=WKE.

[84] *Cfr*: STS 173/2018, de 11 de abril, ES:TS:2018:1385, Fj.7.

ámbito de estos artículos la actuación en canales cerrados de comunicación, y siendo por tanto la que precisa autorización judicial, ya que es evidente que lo que es público es accesible a todos sin necesidad de autorización alguna. En este sentido se ha pronunciado el TS en varias de sus sentencias, como en la STS 739/2008, en la que expresaba que "no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encuentran protegidos por el art. 18.3 CE[85]".

Así lo ha seguido reiterando años después, como en la STS 173/2018, 11 de abril, en la que se hace uso de esta diligencia en la investigación de un delito de pornografía infantil, y en la que el tribunal, haciendo alusión a la sentencia citada, expresa los siguiente: "no precisándose autorización judicial para conseguir lo que es público cuando el propio usuario de la red ha introducido dicha información en la misma"[86].

De acuerdo con el apartado sexto del artículo mencionado, para que pueda llevarse a cabo esta diligencia será necesario que así lo autorice el Juez de instrucción competente, teniendo que ponerlo inmediatamente en conocimiento del juez competente.

Además, para que pueda ser acordada la práctica de esta medida es requisito necesario que nos encontremos ante una investigación de delitos cometidos por la delincuencia organizada. El artículo hace referencia a "los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a". Los delitos correspondientes al apartado 4 son:

> "a) Delito de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el art. 156 bis CP; b) Delito de secuestro de personas previsto en los arts. 164 a 166 CP; c) Delito de trata de seres humanos previsto en el art. 177 bis CP; d) Delitos relativos a la prostitución previstos en los arts. 187 a 189 CP; e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los arts. 237, 243, 244, 248 y 301 CP; f) Delitos relativos a la propiedad intelectual e industrial previstos en los arts. 270 a 277 CP; g) Delitos contra los derechos de los trabajadores previstos en los arts. 312 y 313 CP; h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el art. 318 bis CP; i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los arts. 332 y 334 CP; j) Delito de tráfico de material

[85] *Cfr*. STS 292/2008, 28 de mayo, ES:TS:2008:3346, FJ 9.

[86] *Cfr*. STS 173/2018, 11 de abril, ES:TS:2018:1385, FJ.7.

nuclear y radiactivo previsto en el art. 345 CP; k) Delitos contra la salud pública previstos en los arts. 368 a 373 CP; l) Delitos de falsificación de moneda, previsto en el art. 386 CP, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el art. 399 bis CP; m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los arts. 566 a 568 CP; n) Delitos de terrorismo previstos en los arts. 572 a 578 CP; o) Delitos contra el patrimonio histórico previstos en el art. 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando."

Por otro lado, los delitos a los que se refiere el artículo 588 ter a, son los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Dado el notable aumento del uso de internet como ayuda para la perpetración de estos delitos, el agente encubierto informático ha sido una medida de gran utilidad para su investigación. Como ejemplo de ello, quiero mencionar las sentencias STS 767/2007 de 3 octubre y la STS 345/2019, de 7 de febrero[87].

En la primera, el agente encubierto informático, en el curso de una investigación de un delito de pornografía infantil, mantiene conversaciones con el investigado, a través de Messenger, consiguiendo que el investigado que le proporcionara varios archivos de contenido pornográfico y le confiese la existencia de un "foro denominado la gran familia en el que un grupo organizado de personas mayores de edad fijaban sus encuentros con la participación de sus hijos menores para mantener con éstos relaciones sexuales"[88].

En la segunda, un agente de la Policía Judicial actúa como agente encubierto informático, en el curso de una investigación por delito de terrorismo, para infiltrarse en el ámbito reservado de las redes sociales del investigado. El agente conversó con el investigado a través de Messenger, creando con él una relación de confianza, que les permitió acceder al contenido privado del acusado, pudiendo así demostrar su vinculación con el DAESH.

Para concluir la explicación acerca del agente encubierto informático añadir que, en virtud del artículo 282, apartado sexto, el agente también puede ser autorizado "para intercambiar o enviar por sí mismo archivos de contenido ilícito o para analizar los resultados de los algoritmos aplicados para la identificación de tales archivos", y según el apartado 7 del

[87] *Cfr*: STS 767/2007 de 3 octubre, ES:TS:2007:6202; 345/2019, de 7 de febrero, ES:TS:2019:2393.

[88] *Cfr*: STS 767/2007 3 octubre, ES:TS:2007:6202, Fj.4.

mismo, el juez también podrá autorizar "la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio".

En definitiva, es innegable la importancia y la eficacia de la figura del agente encubierto informático para la investigación de determinados delitos.

4. CONCLUSIONES

1) Como hemos podido observar a lo largo del trabajo, en los últimos años se ha experimentado un notable incremento en el uso de las tecnologías y la informática. Estos avances tecnológicos se han visto presentes en muchos ámbitos de nuestra vida, hasta el punto de que se han visto también reflejados tanto la perpetración de delitos como en la evolución del Derecho.

   La incidencia de esta evolución tecnológica en el Derecho se muestra especialmente en materia de investigación criminal, ya que ha supuesto la necesidad de adaptar las medidas de investigación a estas nuevas circunstancias, dando lugar así al nacimiento de unas diligencias de investigación diferentes a las tradicionales, las diligencias de investigación tecnológicas.

2) Hasta el año 2015 no se ha producido la reforma de la Ley de Enjuiciamiento Criminal, y la consiguiente regulación de estas diligencias de investigación tecnológica, por lo que es indudable la importancia que ha tenido la jurisprudencia en esta materia, que durante años ha ido supliendo las carencias de la ley.

   La jurisprudencia juega un papel determinante en el estudio de esta materia, pero no solo por haberse encargado de suplir estas carencias, sino también porque ha servido de guía para el desarrollo de la reforma, y porque actualmente sigue perfilando detalles de la misma.

3) A pesar este encomiable esfuerzo jurisprudencial, tampoco se puede negar la necesidad de un marco legal claro, que ha venido patrocinado por la LO 13/2015, de modificación de la LECrim, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

   Con esta reforma se ha terminado finalmente con el vacío normativo existente, vacío que, en tantas ocasiones ha denunciado el Tribunal Europeo de Derechos Humanos,

y, con ella también, se ha proporcionado al Derecho español una regulación lo suficientemente clara y precisa para cumplir con las garantías procesales exigibles.

4) Estas nuevas diligencias de investigación tecnológica suponen una gran incidencia en derechos fundamentales del investigado, tales como, el derecho al secreto de las comunicaciones, el derecho a la intimidad, el derecho a la inviolabilidad del domicilio, o el derecho a la protección de datos, regulados en el artículo 18CE.
   Es por ello por lo que, tanto la ley como la jurisprudencia, precisan para su adopción, en la mayoría de los casos, la correspondiente autorización judicial. La necesidad de este control judicial, tanto para adoptar la medida, como para su posterior desarrollo, no es otra que evitar la interferencia desproporcionada de los poderes públicos en la privacidad y en los derechos fundamentales de los investigados.

5) Dada la presencia que tienen hoy en día los dispositivos informáticos en nuestras vidas, es evidente que accediendo a ellos se puede acceder a infinidad de datos, de diferente naturaleza, verdaderamente relevantes sobre la vida privada de las personas. Por ello, se ha considerado el registro remoto sobre equipos informáticos como una medida especialmente invasiva para los derechos fundamentales del investigado, lo que habrá de tenerse en cuenta a la hora de su adopción y control.

6) Por otro lado, merece mención aparte, la figura del agente encubierto informático, otra medida de investigación novedosa introducida también por la LO 13/2015. Esta figura guarda bastante relación con el agente encubierto tradicional, pero, en este caso, adaptada a esta presencia de la informática en la comisión de delitos. Con esta figura se proporciona a los agentes de la policía, para la investigación de determinados delitos cometidos por organizaciones criminales, la posibilidad también de infiltrarse, pero en este caso, en la red, concretamente en canales cerrados de comunicación. También cabe destacar sobre esta medida la novedosa posibilidad de autorizar a los agentes para que intercambien y envíen archivos de contenido ilícito.

7) Para concluir quiero destacar, que no hay que olvidarse de la doble cara que tienen estas diligencias de investigación. Por un lado, no se puede negar la evidente eficacia y utilidad que tienen todas estas diligencias para la investigación de delitos, pero, a su vez, tampoco se puede negar el gran perjuicio que pueden suponer, puesto que

tampoco se puede negar la incidencia, en mayor o en menor medida, en los derechos fundamentales de la persona investigada. Y no solo eso, sino que muchas veces es inevitable que estas medidas afecten también a terceros totalmente ajenos a la investigación. Por todo ello, va a ser necesario, en la práctica de estas medidas, un control judicial adecuado que permita cumplir con las exigencias de la ley y proporcione las garantías necesarias.

5. BIBLIOGRAFÍA

ARMENTA DEU, Teresa. *Lecciones de derecho procesal penal.* Madrid: Marcial Pons, 2019.

ARRABAL PLATERO, Paloma. La prueba tecnológica: aportación, práctica y valoración. Valencia: Tirant lo Blanch, 2020.

ASENCIO MELLADO, José María. *Derecho procesal penal.* Valencia: Tirant lo Blanch, 2019.

BACHMAIER WINTER, Lorena. "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015". *Boletín del Ministerio de Justicia*, año 71, n. º 2195, 2017.

Circular 1/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal (BOE n. º 70 de 22 de marzo de 2019). Referencia: BOE-A-2019-4240.

Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. (BOE núm. 70, de 22 de marzo de 2019). Referencia: BOE-A-2019-4241.

Circular 3/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (BOE núm. 70 de 22 de marzo de 2019). Referencia: BOE-A-2019-4242.

Circular 4/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (BOE núm. 70 de 22 de Marzo de 2019). Referencia: BOE-A-2019-4243.

Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos (BOE núm. 70, de 22 de marzo de 2019). Referencia: BOE-A-2019-4244.

Circular 5/2015, de 13 de noviembre, de la fiscalía General del Estado, sobre los plazos máximos de la fase de instrucción. Referencia: FIS-C-2015-00005

GASCÓN INCHAUSTI, Fernando. *Infiltración policial y "agente encubierto"*. Comares: Granada, 2001.MONTERO AROCA, Juan. *Derecho jurisdiccional III. Proceso penal.* Valencia: Tirant lo Blanch, 2019.

MORENO CATENA, Víctor. *Derecho procesal penal.* Valencia: Tirant lo Blanch, 2019.

SÁNCHEZ GÓMEZ, Raúl. "*La Ley Penal*" n.º 118, Sección Estudios, Enero-Febrero 2016, Editorial LA LEY.

LEGISLACIÓN

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

ANEXO JURISPRUDENCIAL

TRIBUNAL SUPREMO

STS 412/2011, de 11 de mayo. ES: TS: 2011:3088

STS 985/2009, de 13 de octubre. ES: TS: 2009:6139

STS 71/2017, de 8 de febrero. ES: TS: 2017:441

STS 85/2017, de 15 de febrero ES: TS: 2017: 476

STS 993/2016, de 12 de enero de 2017, ES: TS: 2017: 81

STS 982/2016, de 11 de enero de 2017, ES: TS: 2017: 40

STS 279/2017, de 19 de abril. ES: TS: 2017:1642

STS 373/2016, de 3 de mayo. ES: TS: 2016:1942

STS 104/2011, de 1 de marzo. ES: TS: 2011:1316

STS 441/2017, de 8 de febrero, ES:TS:2017:441

STS 276/96 de 2 de abril, ES:TS:1996:2030

STS 792/2007 de 30 de mayo, ES:TS:2007:6384

STS 457/2010 de 25 de mayo, ES:TS:2010:2665

STS 426/2016 de 19 de mayo, ES:TS:2016:2149

STS 71/2017, de 8 de febrero, ES:TS:2017:441

STS 173/98, de 10 de febrero, ES:TS:1998:853

STS 354/2003, de 13 de marzo, ES:TS:2003:1724

STS 419/2013, de 14 de mayo, ES:TS:2013:2450

STS 793/2013, de 28 de octubre, ES:TS:2013:5249
STS 517/2016, de 14 de junio, ES: TS: 2016: 2895
STS 793/2013, de 28 de octubre, ES: TS: 2013: 5249
STS 985/2009, de 13 de octubre, ES:TS:2009:6139
STS 968/1998, de 17 julio, ES:TS:1998:4822
STS 67/2014, de 28 enero, ES:TS:2014:558
STS 409/2014, de 21 de mayo, ES:TS:2014:2209
STS 200/2017, de 27 de marzo, ES:TS:2017:1069
STS 272/2017, de 18 de abril, ES: TS: 2017: 1594
STS 157/1999 de 30 enero, ES:TS:1999:503
STS 968/1998 de 17 julio, ES:TS:1998:4822
STS 223/1998 de 3 septiembre, ES:TS:1998:5067
STS 1733/2002 de 14 de octubre, ES:TS:2002:6716
STS 299/2006 de 17 marzo, ES:TS:2006:1517
STS 597/2010 de 2 de junio, ES:TS:2010:3136
STS 1140/2010 de 29 de diciembre, ES:TS:2010:7184
STS 329/2016, 20 de abril, ES: TS: 2016: 1709
STS 354/2003, 13 de marzo, ES:TS:2003:1724
STS 610/2016, de 7 de julio, ES: TS: 2016: 3621
STS 204/2016, 10 de marzo, ES: TS: 2016: 1218
STS 342/2013, de 17 de abril, ES: TS: 2013: 2222
STS 786/2015, de 4 de diciembre, ES: TS: 2015: 5362
STS 204/2016, de 10 de marzo, ES: TS: 2016: 1218
STS 342/2013, de 17 de abril, ES: TS: 2013: 2222
STS 864/2015, de 10 de diciembre, ES: TS: 2015: 5809
STS 173/2018, de 11 de abril, ES:TS:2018:1385
STS 292/2008, 28 de mayo, ES:TS:2008:3346
STS 173/2018, 11 de abril, ES:TS:2018:1385
STS 767/2007 3 octubre, ES:TS:2007:6202

TRIBUNAL CONSTITUCIONAL

STC 14/2001, de 29 de enero, ES:TC:2001:14
STC 126/2000, de 16 de mayo, ES:TC:2000:126
STC 299/2000, de 11 de diciembre, ES:TC:2000:299
STC 230/2007, de 5 de noviembre, ES:TC:2007:230

STC 115/2013, de 9 de mayo, ES:TC:2013:115

STC 145/2014, de 22 de septiembre, ES:TC:2014:145

STC 26/2006, de 30 enero, ES: TC: 2006: 26

STC 123/2002, de 20 de mayo, ES: TC: 2002: 123

STC 39/2016, de 3 de marzo, ES: TC: 2016: 39

STC 206/2007, de 24 de septiembre, ES: TC: 2007: 206

STC 173/2011, 7 de noviembre, ES: TC: 2011: 173

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

STEDH de 30 de julio de 1988, caso *Valenzuela Contreras c. España*, CE:ECHR:1998:0730JUD002767195

STEDH de 24 de abril de 1990, *caso Kruslin c. Francia*, CE:ECHR:1990:0424JUD001180185

STEDH de 24 de abril de 1990, *caso Huvig c. Francia*, CE:ECHR:1990:0424JUD001110584

STEDH de 26 de Septiembre de 2006, caso *Abdulkadir Cobán c. España*, CE:ECHR:2006:0925DEC001706002

STEDH caso *Uzun c. Alemania,* de 2 de septiembre de 2010, CE:ECHR:2010:0902JUD003562305

STEDH de 18 de febrero de 2003, Caso *Prado Bugallo c. España, CE:ECHR:2003:0218JUD005849600*

STEDH de 31 de mayo de 2005, caso *Vetter c. Francia, CE:ECHR:2005:0531JUD005984200*

STEDH de 6 de septiembre de 1978, caso *Klass y otros c. Alemania, CE:ECHR:1978:0906JUD000502971*

STEDH de 22 de mayo de 2008, caso Iliya Stefanov c. Bulgaria, CE:ECHR:2008:0522JUD006575501.

TRIBUNAL SUPERIOR DE JUSTICIA

STSJ Cataluña núm. 11/2011, de 5 de mayo, ES: TSJCAT: 2011: 5794

AUDIENCIA PROVINCIAL

SAP Madrid de 4 de junio de 2002, ES:APM:2002:7155

SAP de A Coruña, ES:APC:2019:281

JUZGADO DE LO PENAL

SJP de Córdoba 19/2020, de 14 de abril, ES:JP:2020:19

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

STJUE de 2 de octubre de 2018, asunto C-207/16, ECLI: EU:C:2018:788